

[0231] The secure communication control unit 62 acquires the UIM public key corresponding to the destination UIM 12 from the authentication server (refer to the first embodiment), and encrypting the program by the UIM public key, sends it to the UIM 12. In the UIM 12, the program is decrypted using the UIM private key paired with the UIM public key. Once the decryption is successful, a program in a common text is obtained. The UIM 12 writes this program in the basic block 40-X (step S147). The UIM 12 determines the basic block 40-X by the same algorithm as used by the program information storage unit 52 in the distribution management server 16A. In step S147, therefore, the same basic block 40-X is obtained as determined in step S134 of Fig. 24. Alternatively, the registration completion notice transmitted from the distribution management server 16A in step S139 of Fig. 24 may contain the information specifying the unoccupied basic block 40-X determined in step S134, and in step S147 of Fig. 25, the program is stored in the basic block 40-X specified by the particular information.

[0232] The UIM 12, at the end of the program write operation, transmits a write end notice to the secure communication control unit 62 of the distribution management server 16 (step S148). This write end notice contains the information for specifying the basic block 40-X in which the program is written.

[0233] When the secure communication control unit 62 of the distribution management server 16 receives the write end notice, the user information storage unit 51 sends an activation request to the contents server 19 in order to request the permission for execution of the program written in the UIM 12 (step S149).

[0234] The contents server 19 that has received this activation request sends an activation permission to the user information storage unit 51 (step S150).

[0235] The user information storage unit 51 that has received the activation permission sends an activation instruction to the UIM 12 (step S151).

[0236] In the UIM 12, upon receipt of the activation instruction, the activation flag corresponding to the basic block 40-X in which the program is written turns from "0" to "1", after which the execution of the program in the particular basic block becomes possible.

[0237] The UIM 12, at the end of the program activation, transmits an activation acknowledgment notice indicating the end of the program activation to the user information storage unit 51 of the distribution management server 16A, together with the information specifying the program (for example, the information specifying the basic block 40-X) (step S152).

[0238] The user information storage unit 51, upon receipt of the activation acknowledgment notice from the UIM 12 of the user k, determines an area of the real distribution information storage unit 54 of the individual user information storage unit 53-k corresponding to the basic block 40-X. In this area, the pointer data corresponding to the program written in the basic block 40-X is al-

ready written in the UIM 12 of the user k. In this area, the information to the effect that the activation is complete is written in such a form that a given pointer coexists. As the result of this operation, the distribution management server 16A can grasp whether the activation has been performed for the basic blocks 40-1 to 40-7 of all the UIMs 12 by accessing each area of the user information storage unit 51.

[0239] The user information storage unit 51, at the end of the operation for writing the information to the effect that the activation is complete, notifies the mobile terminal 11 that the registration is complete as a program list, and subsequently notifies that the program can be executed, while at the same time ending the process (step S153).

[0240] The distribution management server 16A notifies the contents server 19 that the activation of the program is completed (step S154).

[2.3.1.2] Registration of in UIM basic block (in the case where the distribution management server holds the program proper)

[0241] In the example of operation shown in Fig. 25, the program proper, of which the distribution is desired by the user, is not stored in the distribution management server 16A but in the contents server 19. In the operation example shown in Fig. 26, in contrast, the program proper of which the distribution is desired by the user is stored in the distribution management server 16A. The operation example shown in Fig. 25 will be explained below.

[0242] The user accesses the registration list received from the distribution management server 16A, and performs the operation for selecting the desired program. A distribution request containing the pointer in the registration list corresponding to the particular program is sent from the mobile terminal 11 to the user information storage unit 51 of the distribution management server 16A (step S161).

[0243] The user information storage unit 51, upon receipt of the distribution request from the mobile terminal 11 of the user k, reads the pointer data for specifying the place of storage of the URL of the program or the program proper of which the distribution is requested, from that area of the real distribution information storage unit 54 of the individual user information storage unit 53-k which corresponds to the pointer in the registration list contained in the distribution request. The distribution request containing this pointer data is sent to the program information storage unit 52 (step S162).

[0244] The program information storage unit 52 accesses the area designated by the pointer data in the distribution request. In the case where the program proper is stored in the particular area, the secure communication control unit 62 requests the authentication server 18 to issue a certificate, i.e. sends a request for the UIM public key required for encrypting the program

proper and sending it to the UIM 12 of the user k (step S163).

[0245] In the case where the program corresponding to the distribution request is a program permitted to write in the UIM 12, the authentication server 18 sends the UIM public key to the secure communication control unit 62 (step S164).

[0246] The secure communication control unit 62 receives this UIM public key, and upon determination that the key is legitimate, encrypts the program to be distributed using the UIM public key, and thus generates a program with certificate.

[0247] When the user performs the operation at the mobile terminal 11 to permits the program distribution, the secure communication control unit 62 of the distribution management server 16A sends a program with certificate to the UIM 12 of the mobile terminal 11 (step S165).

[0248] The UIM 12 has stored therein a UIM private key paired with the UIM public key and using this UIM private key, decrypts the program. The same program is written in the basic block 40-X.

[0249] The subsequent operation is similar to the corresponding operation shown in Fig. 25. In Fig. 26, steps S166 to S171 correspond to steps S148 to S153 in Fig. 25.

[2.3.1.3] Registration in UIM basic block (In the case where the distribution management server holds the program proper, and the secure communication control unit holds the UIM public key)

[0250] It may happen that when the mobile terminal 11 sends a distribution request to the distribution management server 16A, the secure communication control unit 62 of the distribution management server 16A holds the UIM public key of the UIM 12 to which the program is to be distributed. Such a phenomenon may occur, for example, in the case where programs are distributed to the same UIM 12 within a short time. Fig. 27 shows an example of the operation performed in such a case. In this operation example, when a program proper corresponding to the distribution request is found, the program is encrypted using the UIM public key held in the secure communication control unit 62 and written in the UIM 12. The operation shown in Fig. 27 is similar to the operation shown in Fig. 26, except that the operation corresponding to steps S163 and S164 for acquiring the UIM public key from the authentication server 18 is lacking. Steps S181, S182, S183 to S189 in Fig. 27 correspond to steps S161, S162, S165 to S171, respectively, in Fig. 26.

[2.3.1.4] Registration in UIM free basic block

[0251] The user, by operating the mobile terminal 11, can register a program in the free basic block 40-F1 of the UIM 12. This operation is shown in Fig. 28.

[0252] In the case where a program is registered in the free basic block 40-F1 of the UIM 12, the user operates the mobile terminal 11 so that the desired contents server 19X is accessed and a request for distributing the desired program is sent to it (step S191).

[0253] The contents server 19X that has received this distribution request distributes the requested program to the secure communication control unit 62 of the distribution management server 16A (step S192).

[0254] The user performs the operation to permit the distribution to the free basic block 40-F1, and the information indicating the particular operation is sent from the mobile terminal 11 to the distribution management server 16A. Then, the secure communication control unit 62 distributes the program to the UIM 12 of the mobile terminal 11 (step S193). This program may be sent in encrypted form or without encryption. The UIM 12 writes this program in the free basic block 40-F1.

[0255] The UIM 12, at the end of the program write operation, transmits a write end notice to the distribution management server 16 (step S194).

[0256] The user information storage unit 51 of the distribution management server 16 receives the write end notice from the UIM 12 of the user k and updates the information including the number of distribution sessions stored in the area of the user individual information storage unit 53-k corresponding to the free basic block 40-F1 (step S195).

[0257] Once this update operation is completed, the user information storage unit 51 sends to the UIM 12 an activation instruction for the program written in the free basic block 40-F1 (step S196).

[0258] The UIM 12, in compliance with this instruction, completes the program activation and transmits to the user information storage unit 51 of the distribution management server 16 an activation response notice indicating that the activation of the program in the free basic block 40-F1 is completed (step S197).

[0259] The user information storage unit 51, upon receipt of the activation response notice from the UIM 12 of the user k, registers the information that the activation is complete, in the area of the individual user information storage unit 53-k corresponding to the free basic block 40-F1. The user information storage unit 51 notifies, in the form of program list, the mobile terminal 11 that the registration is complete, thereby terminating the process (step S198).

[2.3.1.5] Program deletion from user information storage unit

[0260] Now, the process for deleting the program registered in the user information storage unit 51 will be explained with reference to Fig. 29.

[0261] The user, by performing a predetermined operation, can display the registration program list received from the distribution management server 16A, on the display unit 21. Under this condition, the user spec-

ifies the desired program and instructs to delete the program in the distribution management server 16A. A program registration delete request containing the information for specifying what is to be deleted is sent to the user information storage unit 51 of the distribution management server 16A (step S201).

[0262] In the case where the program to be deleted is already deleted from any one of the basic blocks 40-1 to 40-7 of the UIM 12, the user information storage unit 51 sends a cancel request indicating the desire of the user to cancel the utilization of the program, to the contents server 19 from which the particular program is distributed (step S202). In the case where a program to be deleted remains undeleted in any one of the basic blocks 40-1 to 40-7 of the UIM 12 on the other hand, the process for deletion of the program from the basic blocks 40-1 to 40-7 described later, is carried out at the same time under the guidance of the distribution management server 16A.

[0263] The contents server 19, upon receipt of the cancel request, sends a cancel permission notice to the user information storage unit 51 of the distribution management server 16A (step S203).

[0264] The user information storage unit 51, upon receipt of the cancel permission notice, deletes the information on the program of which the deletion is requested in step S201, and sends the registered program list after deletion to the mobile terminal 11 (step S204).

[2.3.16] Program deletion from UIM basic block

[0265] Now, the process for deleting a program from the basic blocks 40-1 to 40-7 of the UIM 12 will be explained with reference to Fig. 30.

[0266] The user, by performing a predetermined operation, can display on the display unit 21 the registered program list transmitted already to the mobile terminal 11. Under this condition, assume that the user specifies the desired program and gives an instruction to delete it. One of the basic blocks 40-1 to 40-7 of the UIM 12 where the program to be deleted is stored is determined, and a deletion request containing the information specifying the particular basic block is transmitted from the mobile terminal 11 to the user information storage unit 51 of the distribution management server 16A (step S211).

[0267] The user information storage unit 51, upon receipt of the deletion request, sends a deletion permission notice to the UIM 12 (step S212).

[0268] The UIM 12, upon receipt of the deletion permission notice, deletes the program specified by the user in step S211 from the basic block, and sends a deletion end notice to the user information storage unit 51 (step S213).

[0269] As a result, the user information storage unit 51 deletes the information on the corresponding program under the control of the transmission control unit 61, and gives a deletion notice to the contents server 19

(step S214).

[0270] Also, the user information storage unit 51 notifies the mobile terminal 11 that the deletion is complete in the form of a program list, thereby ending the process.

[2.3.1.6.1] The case in which the program deletion from basic block is carried out at the same time under the guidance of distribution management server.

[0271] As described above, if the process for deleting a program from the basic blocks 40-1 to 40-7 is carried out at the same time as the deletion of the program from the user information storage unit 51 under the guidance of the distribution management server, the user information storage unit 51 of the distribution management server sends a deletion instruction to the UIM by specifying the program of which deletion is requested, in place of the process of steps S211 and S212 described above.

[2.3.1.7] The case in which use of user information storage unit is prohibited.

[0272] According to this embodiment, a deactivation process for the user information storage unit can be executed for preventing the user from using the user information storage unit 51. This deactivation process for the user information storage unit is carried out, for example, in the case where the distribution management server 16A stops the service temporarily, or the service of the distribution management server 16A to the user is temporarily suspended at the request of the contents provider holding the contents server 19. Once this deactivation process for the user information storage unit is carried out, the distribution of the programs registered in the user information storage unit 51 to the UIM 12 is prohibited and so is the deletion of the programs registered in the UIM 12.

[0273] Now, with reference to Fig. 31, the deactivation process for the user information storage unit will be explained. The following description concerns the case in which the contents server 19 requests the deactivation process for the user information storage unit.

[0274] First, the contents server 19 sends a user information storage unit deactivation request to the user information storage unit 51 of the distribution management server 16A (step S221).

[0275] The user information storage unit 51, upon receipt of the user information storage unit deactivation request, is prohibited from use (deactivated state), and sends a user information storage unit deactivation permission notice to the contents server 19 (step S222).

[0276] Then, the user information storage unit 51 sends to the mobile terminal 11 a user information storage unit deactivation notice to the effect that the use of the user information storage unit 51 has been prohibited (step S223).

[0277] As a result, the user of the mobile terminal 11

can confirm that the use of the user information storage unit 51 has been prohibited.

[2.3 1.7.1] The case in which the user information storage unit is deactivated by distribution management server

[0278] In the case where the user information storage unit is deactivated by the distribution management server 16A by itself, the user information storage unit 51 is prohibited from use (deactivated) and sends a user information storage unit deactivation notice to the mobile terminal 11 indicating that the use of the user information storage unit 51 is prohibited (step S223).

[2.3 1.8] The case in which the use of the program stored in UIM basic block is prohibited

[0279] Now, the process for prohibiting the use of a program stored in the basic blocks 40-1 to 40-7 or the free basic block 40-F1 of the UIM 12 will be explained with reference to Fig. 32.

[0280] This process is carried out in the case where the mobile terminal 11 is stolen or the contents provider requests the user to prohibit the use thereof. Once this process is carried out, the user is prohibited from using the programs stored in the basic blocks (including the free basic block) involved. The description that follows deals with the case in which the user service server 65 in charge of user services, taking an appropriate measure such as when the mobile terminal 11 is stolen, requests the process for deactivating the basic blocks based on the report from the user.

[0281] Fig. 32 shows a sequence of the deactivation process for the basic blocks.

[0282] First, the user service server 65 sends a basic block deactivation request to the user information storage unit 51 of the distribution management server 16A (step S231).

[0283] The user information storage unit 51, upon receipt of the basic block deactivation request, sends a deactivation instruction to the UIM 12 (step S232).

[0284] As a result, the UIM 12 deactivates the basic blocks meeting the basic block deactivation request, and gives a basic block deactivation response indicating that the use of the basic blocks has been prohibited (step S233).

[0285] Then, the user information storage unit 51 gives a basic block deactivation end notice to the user service server 65 indicating that the use of the basic blocks of the UIM 12 has been prohibited (step S234).

[0286] Further, the user information storage unit 51 gives a user information storage unit list to the mobile terminal 11 indicating that the use of the basic blocks (which may include the free basic block) is prohibited, thereby ending the process (step S235).

[2.4] Effects of second embodiment

[0287] As described above according to the second embodiment, programs can be distributed beyond the limit of the number of the storage areas of the storage module (UIM) and the operating convenience on the part of the user is improved.

[0288] Also, the distribution management server can easily manage the activation/deactivation of the program distributed, and the distribution and the activation/deactivation of the program ready for distribution.

[3] Modifications of embodiments

[3.1] First modification

[0289] The foregoing description deals with the case in which a single distribution management server is involved. Nevertheless, a plurality of distribution management servers can be provided for distributed processing.

[0290] In such a case, the programs stored in each UIM and the information on the storage area of each program can be stored in a common database.

[3.2] Second modification

[0291] Apart from the foregoing description, dealing with the case in which the distribution management server is connected directly to a line switching network, the distribution management server can be connected to the line switching network through an internet making up a packet switching network and an internet gateway.

[3.3] Third modification

[0292] Although only the UIM is described above as a storage module, the invention is also applicable to various IC card memories with equal effect. In this case, the storage module can be arranged at a fixed terminal as well as at a mobile terminal.

Claims

1. A program distribution system comprising:

at least a mobile terminal having means for transmitting a program distribution request
a storage module built in or connected to said mobile terminal;
a contents server for receiving said distribution request and transmitting a program to be distributed; and
a distribution management server for receiving said program from said contents server, and only in a case where said contents server is an authorized contents server, transmitting said program received from said contents server to

said storage module built in or connected to said mobile terminal;

characterized in that said storage module includes

a storage unit, and
a control unit for storing in said storage unit said program received from said distribution management server through said mobile terminal and, in compliance with a request, executing said program stored in said storage unit.

2. A program distribution system as set forth in claim 1, further comprising an authentication server for storing a first encryption key unique to said storage module,

characterized in that said control unit of said storage module decrypts said program encrypted by said first encryption key and, only in a case where decryption is successful, said program obtained by decryption is stored in said storage unit.

said contents server, upon receipt of said distribution request, acquires said first encryption key from said authentication server and, using said first encryption key, encrypts said program to be distributed, said contents server further encrypting said program using a second encryption key obtained in advance and transmitting it to said distribution management server, and

said distribution management server decrypts said encrypted program received from said contents server, using said second encryption key, generates a program encrypted only by said first encryption key and, only in a case where said decryption is successful, transmits said program obtained by said decryption to said storage module.

3. A program distribution system as set forth in claim 1, **characterized in that** said storage module stores a program and data used by said program.

4. A program distribution system as set forth in claim 1, **characterized in that** said distribution management server includes a charge processing unit for starting a charge process at a time of distributing a? program to said storage module.

5. A program distribution system as set forth in claim 4, **characterized in that** said charge processing unit charges for rental of said storage module.

6. A program distribution system as set forth in claim 1, **characterized in that** said distribution management server includes a charge processing unit for starting said charge process at a time of holding a program for said storage module.

7. A program distribution system as set forth in claim 6, **characterized in that** said charge processing unit charges for rental of said storage module.

- 5 8. A program distribution system as set forth in claim 1, **characterized in that** said distribution management server transmits an activation instruction to said storage module at the request of another device, and

10 said storage module, upon receipt of said activation instruction, is ready to execute said program stored in said storage module and designated by said activation instruction.

- 15 9. A program distribution system as set forth in claim 1, **characterized in that** said distribution management server transmits a deactivation instruction to said storage module at a request of another device, and

20 said storage module, upon receipt of said deactivation instruction, is ready to execute said program stored in said storage module and designated by said activation instruction.

- 25 10. A program distribution system as set forth in claim 1, **characterized in that** said distribution management server transmits a deletion instruction to said storage module at said request of another device, and

30 said storage module, upon receipt of said deletion instruction, deletes the program designated by said deletion instruction from said storage module.

- 35 11. A program distribution system as set forth in claim 1, **characterized in that** said distribution management server includes means for managing a state of said program in said storage module based on information sent to said storage module.

- 40 12. A program distribution system as set forth in claim 1, **characterized in that** said distribution management server acquires version information for said storage module and determines whether said program is to be distributed or not, based on said version information.

13. A program distribution system as set forth in claim 1, **characterized in that** said mobile terminal includes a first communication unit for communication utilizing a mobile communication network, and a second communication unit different from said first communication unit, and

55 said control unit of said storage module includes means for communication utilizing said second communication unit in accordance with said program stored in said storage module.

14. A program distribution system comprising:

a mobile terminal having means for transmitting a program distribution request;
a storage module built in or connected to said mobile terminal; and
a communication management server for receiving said distribution request; and in a case where a program to be distributed is provided by an authorized contents server, acquiring said program and transmitting it to said storage module built in or connected to said mobile terminal; **characterized in that** said storage module includes
a storage unit, and
a control unit for receiving information through said mobile terminal, storing in said storage unit said information only in a case where said information is a program received from said distribution management server, and executing said program stored in said storage unit, in compliance with a request.

15. A program distribution system as set forth in claim 14, **characterized in that** said distribution management server includes a real distribution information storage unit for storing pointer data for specifying a program sent to said storage module

16. A program distribution system as set forth in claim 15, **characterized in that** said storage unit of said storage module includes a plurality of basic blocks for storing programs, and said real distribution information storage unit of said distribution management server includes a plurality of areas corresponding to a plurality of said basic blocks.

17. A program distribution system as set forth in claim 16, **characterized in that** said distribution management server includes a virtual distribution information storage unit for storing said pointer data for specifying a program capable of being distributed to said storage module but not currently stored in said storage module, and upon receipt of request of distribution, to said storage module, of a program specified by said pointer data stored in said virtual distribution information storage unit, said program is distributed to said storage module and, said pointer data for specifying said program is moved from said virtual information distribution storage unit to said real distribution information storage unit.

18. A program distribution system as set forth in claim 16, **characterized in that** said distribution management server includes a program information storage unit for storing selected one of address information indicating a location of a program capable of being acquired from said contents server and a program

acquired from said contents server and, upon receipt of a request for distribution, to said storage module, of a program specified by said pointer data stored in selected one of said real distribution information storage unit and said virtual storage information storage unit, said program is acquired using said program information storage unit and is distributed to said storage module.

19. A program distribution system as set forth in claim 17, **characterized in that** said mobile terminal includes means for transmitting a menu list request, and

said distribution management server, in compliance with said menu list request, accesses said pointer data stored in said real distribution information storage unit and said virtual distribution information storage unit for said storage module built in or connected to said mobile terminal, generates a list of programs specified by said pointer data, and transmitting said list to said mobile terminal

20. A program distribution system as set forth in claim 14, **characterized in that**

said mobile terminal includes a first communication unit for communication utilizing a mobile communication network, and a second communication unit different from said first communication unit; and

said control unit of said storage module includes means for communication utilizing said second communication unit in accordance with a program stored in said storage module

21. A distribution management server **characterized by** comprising:

means for receiving from a contents server a program encrypted by a first encryption key unique to a destination of distribution and a second encryption key unique to said contents server permitted to distribute said program; and means for decrypting said program received from said contents server to a state encrypted by said second encryption key thereby to generate a program encrypted by only said first encryption key, said program being distributed to said storage module built in or connected to a mobile terminal.

22. A distribution management server **characterized by** comprising:

a program information storage unit for storing selected one of a program acquired in advance from an authorized contents server and address information thereof;
a real distribution information storage unit for

storing pointer data indicating a stored position; in said program information storage unit, of a program which is said program stored in a storage module built in or connected to a mobile terminal, or in a case where address information of said program is stored in said program information storage unit, a selected one of said program and said address information thereof; a virtual distribution information storage unit for storing pointer data indicating said stored position of a program in said program information storage unit, in a case where a program which is said program distributable to said storage module but not currently stored in said storage module, or address information thereof is stored in said program information storage unit; and means for acquiring a program specified by said pointer data stored in said virtual distribution information storage unit, utilizing said program information storage unit in accordance with a request from said mobile terminal, and distributing said program to said storage module, and moving said pointer data to said real distribution information storage unit..

23. A contents server comprising

means for acquiring an encryption key unique to a storage module from an external authentication server upon receipt of a program distribution request from a mobile terminal built in or connected to said storage module; first encryption means for encrypting a program to be distributed, by said first encryption key; second encryption means for encrypting a program obtained by said first encryption means, in such a manner as to be decrypted by the distribution management server for distribution to said storage module; and means for transmitting said program encrypted by said first and second encryption means to said distribution management server.

24. A storage module built in or connected to a mobile terminal, comprising:

a storage unit; and a control unit for receiving an encrypted program from a specific distribution management server through said mobile terminal, decrypting said program by a private key stored in advance, storing said program in said storage unit only in a case where said decryption succeeds and, in response to a request, executing said program stored in said storage unit.

25. A storage module as set forth in claim 24, characterized in that said storage unit includes a plurality

of storage blocks for executing a program, and a storage area for storing an activation flag indicating whether a program stored in each storage block can be executed or not, and

said control unit writes said activation flag in accordance with an instruction received from a distribution management server through said mobile terminal, and in a case where an instruction is given to execute a program stored in any one of basic blocks through said mobile terminal, said control unit determines whether said execution instruction is to be followed or not based on an activation flag corresponding to one of said basic blocks.

26. A program distribution method characterized by comprising:

a step of a mobile terminal transmitting a program distribution request to a contents server, said storage module being built in or connected to said mobile terminal; a step of said contents server receiving said distribution request and transmitting a program to be distributed, to a distribution management server; and a step of transmitting said program to said storage module built in or connected to said mobile terminal to which said distribution request is transmitted, in a case where said contents server transmitting said program is an authorized contents server.

27. A program distribution method comprising:

a step of a mobile terminal transmitting a program distribution request to a contents server, said storage module being built in or connected to said mobile terminal; a step of said contents server receiving said distribution request and acquiring a first encryption key unique to said storage module from an authentication server; a step of said contents server encrypting a program to be distributed, by said first encryption key; a step of said contents server encrypting a program encrypted by said first encryption key, by a second encryption key acquired in advance; a step of said contents server transmitting a program encrypted by said first encryption key and said second encryption key, to a distribution management server; a step of said distribution management server decrypting said program transmitted from said contents server, to a state before said second encryption, and generating a program encrypted only by said first encryption key; and

a step of said distribution management server transmitting a program encrypted only by said first encryption key, to said storage module built in or connected to a mobile terminal to which said distribution request is transmitted.

5

28. A program distribution method comprising:

a step of a mobile terminal transmitting a program distribution request to a distribution management server; a storage module being built in or connected to said mobile terminal;
a step of said distribution management server receiving said distribution request, and determining whether a program to be distributed is a program provided by an authorized contents server or not; and
acquiring said program and transmitting it to a storage module built in or connected to said mobile terminal in a case where said program to be distributed is provided by an authorized contents server.

10

15

20

29. A program distribution method as set forth in claim 28, comprising:

a step of said distribution management server storing a program or address information thereof in storage means in place of said storage module; and
a step of said distribution management server, upon receipt of a program distribution request from said mobile terminal, acquiring a requested program using said storage means and distributing it to said storage module.

25

30

35

30. A program for causing a computer of a distribution management server to execute

a process for receiving from said contents server a program which has been encrypted by a first encryption key unique to a distribution destination and a second encryption key unique to a contents server authorized to distribute a program; and
a process for decrypting a program received from said contents server and thereby restoring said program to a state before the encryption by said second encryption key, thereby generating a program encrypted only by said first encryption key and distributing said program to a storage module built in or connected to a mobile terminal.

40

45

50

31. A program for causing a computer of a distribution management server to execute

a step of receiving a program distribution re-

55

quest from a mobile terminal with a storage module built therein or connected thereto;
a step of determining whether a program to be distributed is provided by an authorized contents server; and
a step of acquiring said program to be distributed and transmitting it to a storage module built in or connected to said mobile terminal in a case where said program is provided by an authorized contents server.

32. A program distribution method as set forth in claim 30, characterized by comprising:

a step of storing a program or the address information thereof in storage means in place of said storage module; and
a step of acquiring a requested program using said storage means and distributing said program to said storage module upon receipt of a program distribution request from said mobile terminal.

33. A program for causing a computer of a contents server to execute:

a process for acquiring, upon receipt of a program distribution request from a mobile terminal with a storage module built therein or connected thereto, an encryption key unique to said storage module from an external authentication server;
the first encryption process for encrypting a program to be distributed, by said first encryption key;
the second encryption process for encrypting a program obtained by said first encryption process, in such a manner as to be decrypted by a distribution management server for distributing a program to said storage module; and
the process for transmitting a program encrypted by said first and second encryption processes to said distribution management server.

34. A program for causing the control unit of a storage module built in or connected to a mobile terminal to execute

a process for receiving an encrypted program from a specified distribution management server through a mobile terminal;
a process for decrypting the received program by a private key stored in advance, and only in a case where said decryption is successful, storing said program in a storage unit; and
a process for executing the program stored in said storage unit, as required.

35. A program for causing a computer of a distribution management server to execute

a process for receiving from a contents server authorized to distribute a program, a program encrypted by a first encryption key unique to a distributee and a second encryption key unique to said contents server; and
a process for decrypting said program received from said contents server, and restoring said program to a state before said encryption by said second encryption key, thereby generating a program encrypted only by said first encryption key, and distributing said program to a storage module built in or connected to a mobile terminal.

36. A program for causing a computer of a distribution management server to execute

a step of receiving a program distribution request from a mobile terminal with a storage module built therein or connected thereto;
a step of determining whether a program to be distributed is provided by an authorized contents server or not; and
a step of acquiring and transmitting a program to be distributed, to a storage module built in or connected to said mobile terminal in the case where said program is provided by an authorized contents server.

37. A program distribution method as set forth in claim 36, **characterized by** comprising:

a step of storing a program or the address information thereof in storage means in place of said storage module; and
acquiring, upon receipt of a program distribution request from said mobile terminal, the requested program utilizing said storage means and distributing said program to said storage module.

38. A program for causing a computer of a contents server to execute:

a process for acquiring an encryption key unique to a storage module built in or connected to a mobile terminal from an external authentication server, upon receipt of a program distribution request from said mobile terminal;
a first encryption process for encrypting a program to be distributed, by said first encryption key;
a second encryption key for encrypting said program obtained by said first encryption process, in such a manner as to be decrypted by a

distribution management server for distributing a program to said storage module; and
a process for transmitting to said distribution management server said program encrypted by said first and said second encryption processes.

39. A program for causing said control unit of a storage module built in or connected to a mobile terminal to execute

a process for receiving an encrypted program from a specified distribution management server through said mobile terminal;
a process for decrypting said received program by a private key stored, and storing said program in a storage unit only in a case where said decryption is successful; and
a process for executing said program stored in said storage unit, as required.

FIG. 1

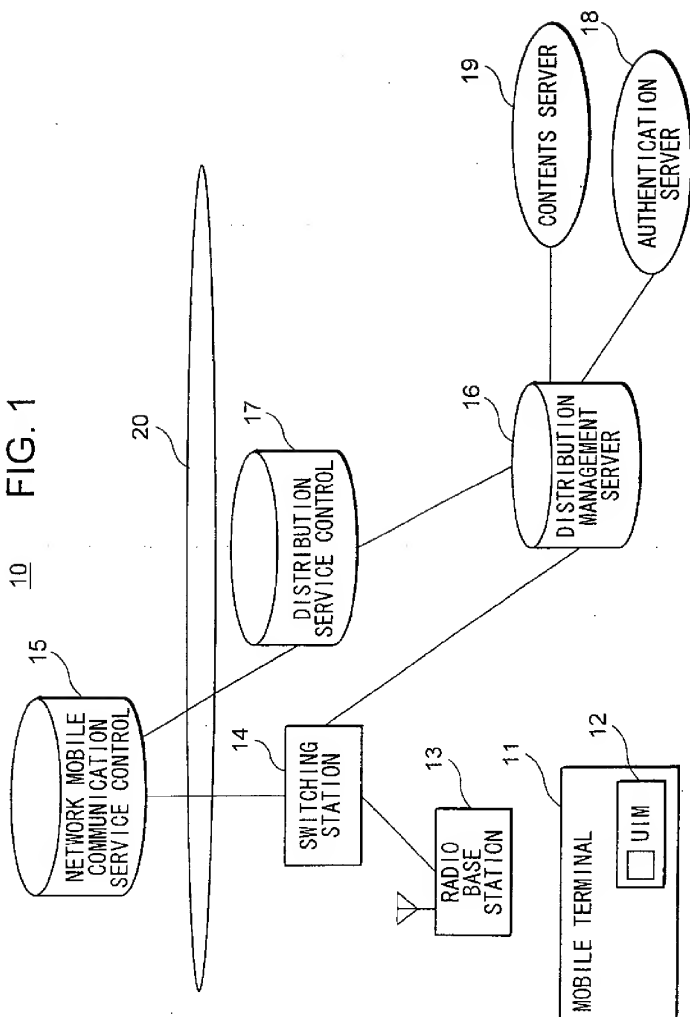


FIG. 2

11

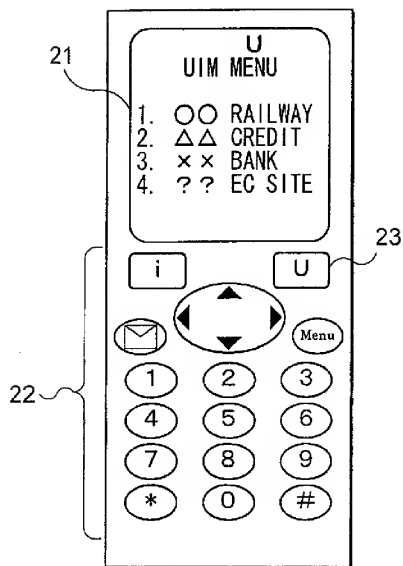


FIG. 3

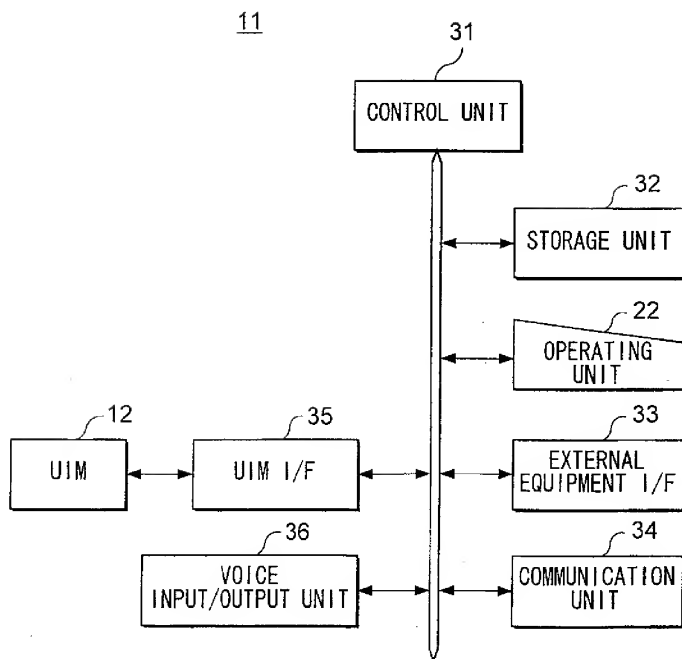
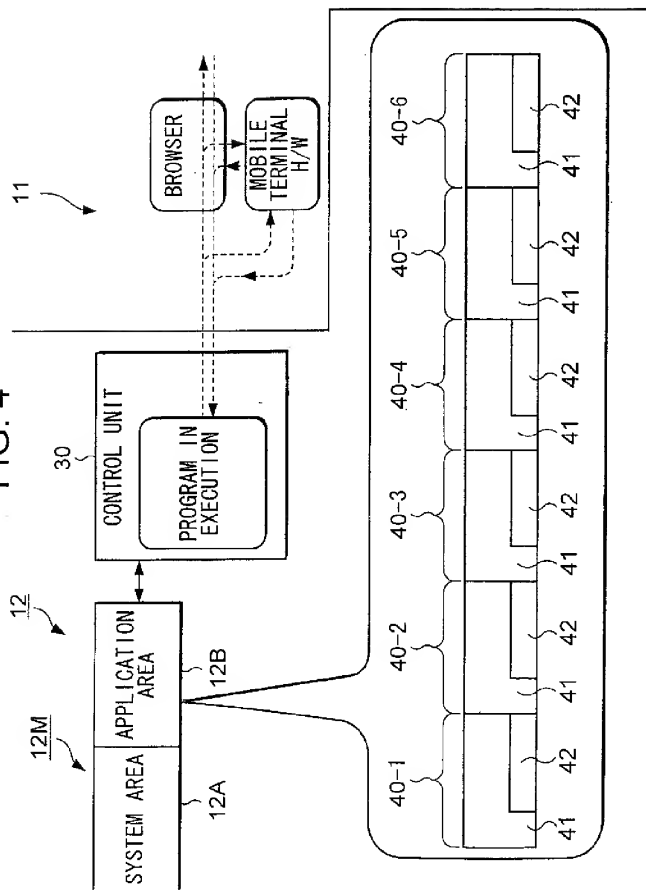


FIG. 4



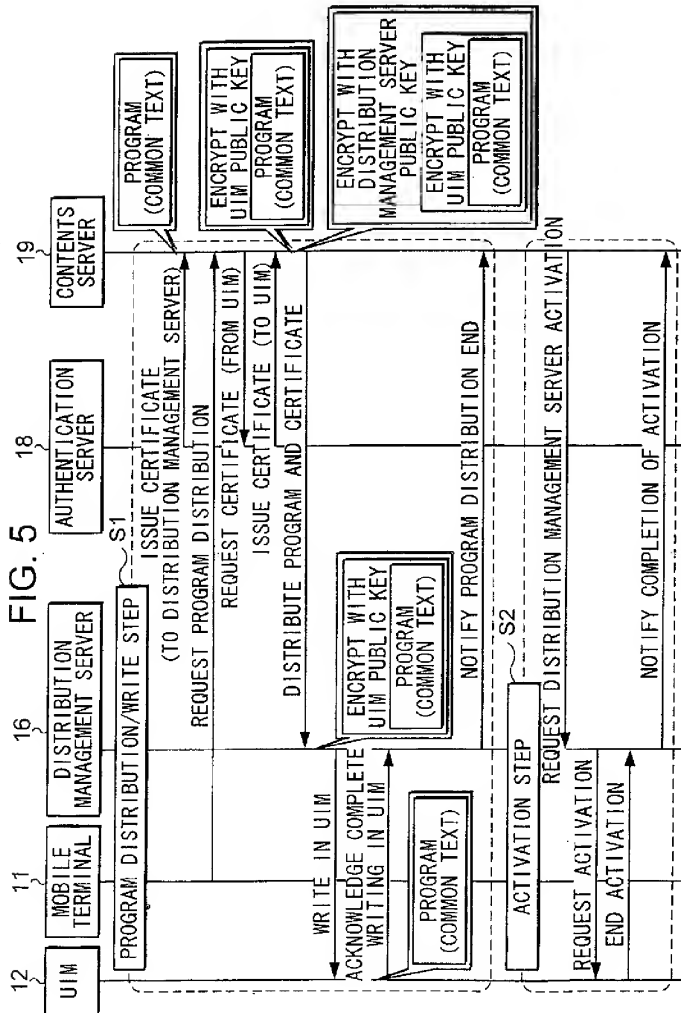


FIG. 6

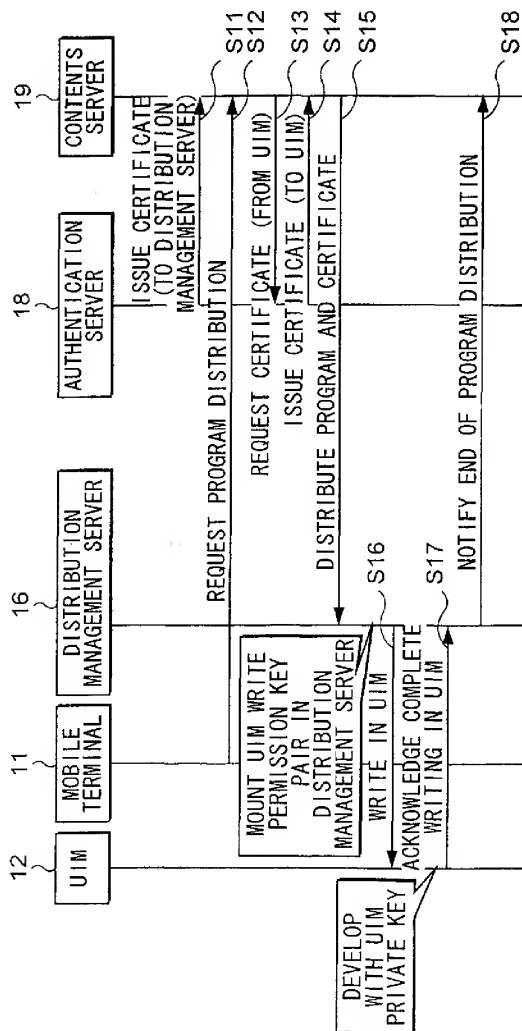


FIG. 7

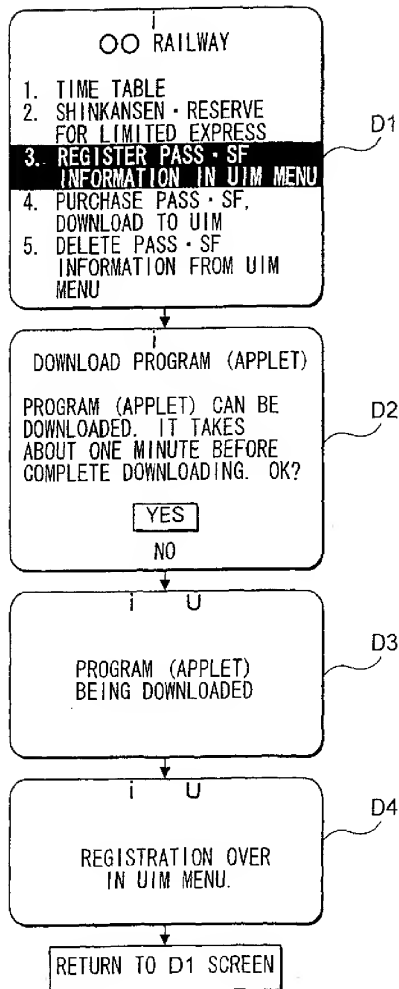


FIG. 8

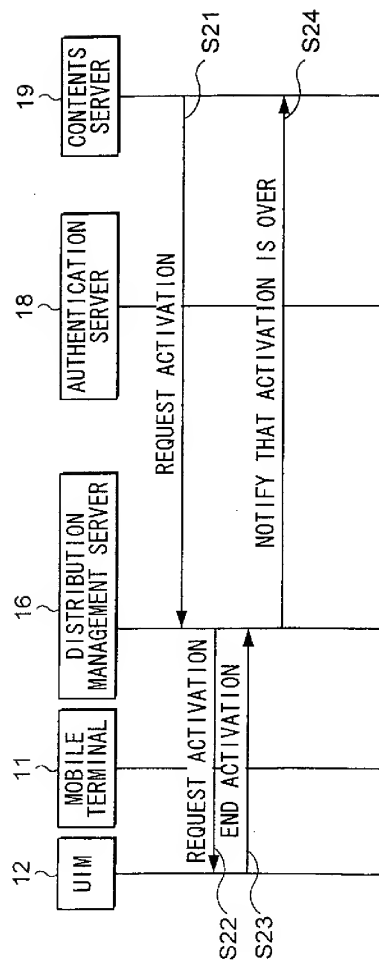


FIG. 9

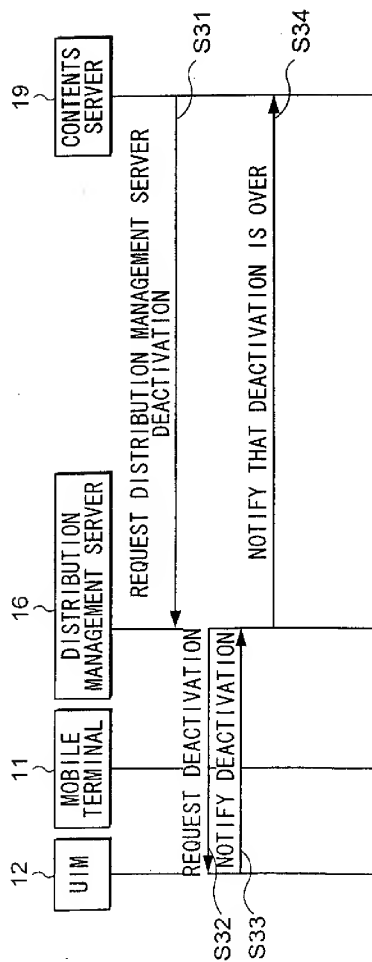


FIG. 10

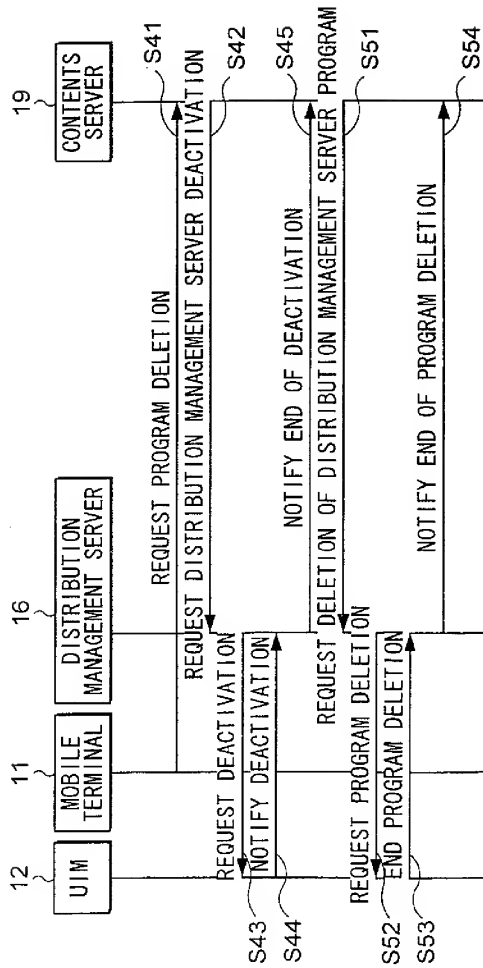


FIG. 11

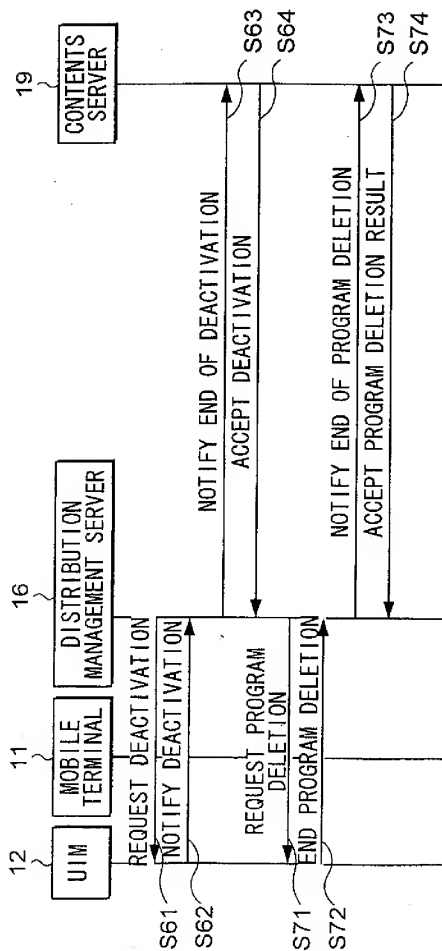


FIG. 12

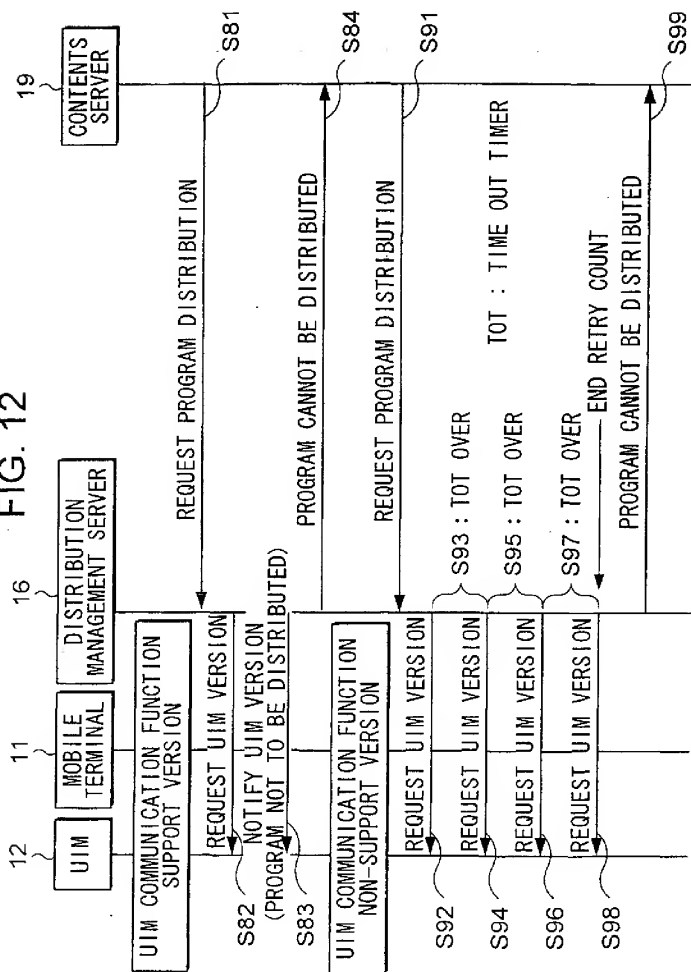


FIG. 13

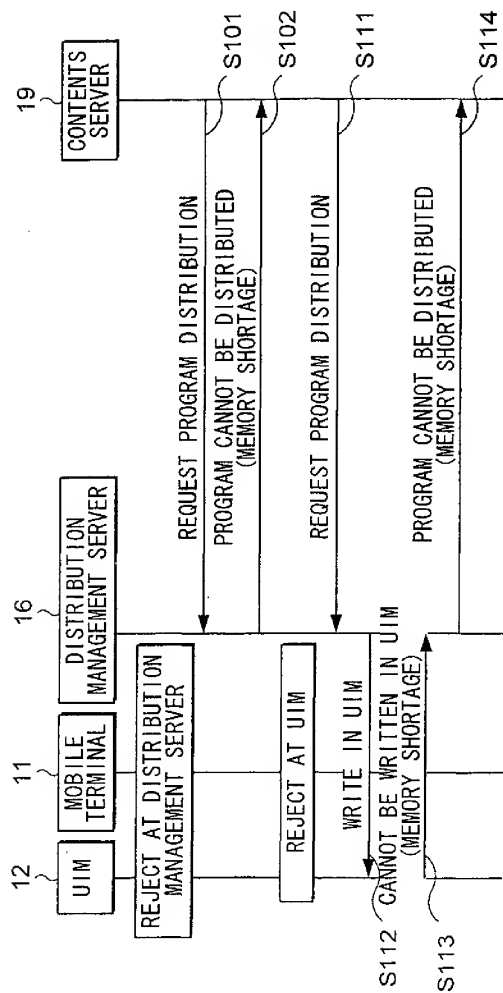


FIG. 14

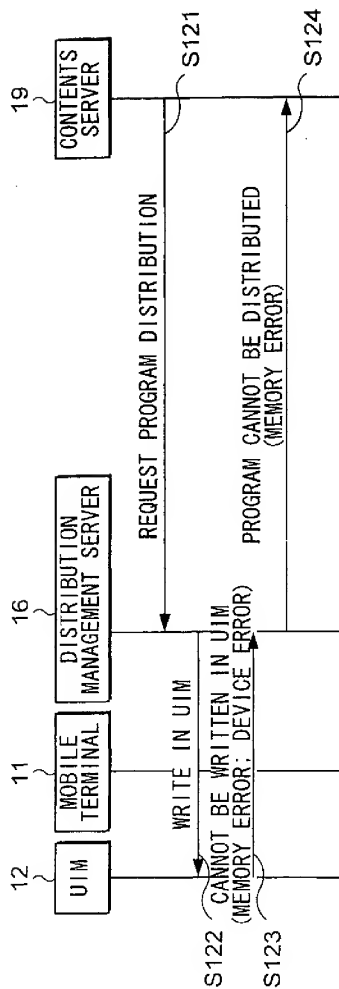


FIG. 15

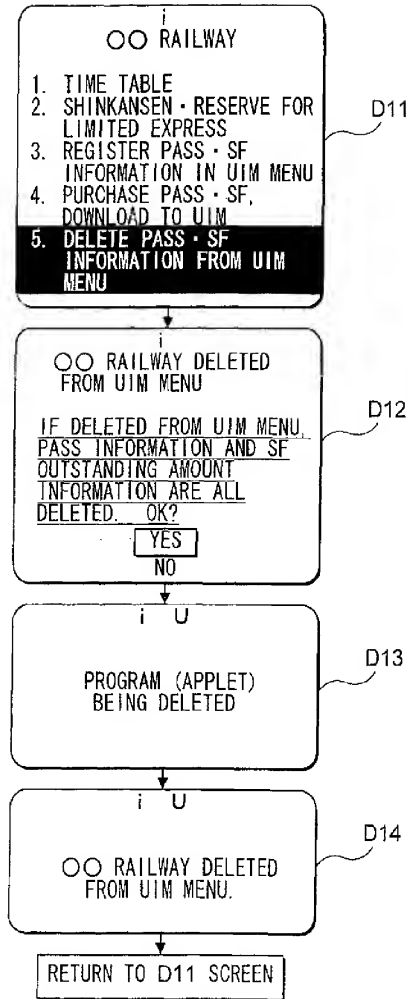


FIG. 16

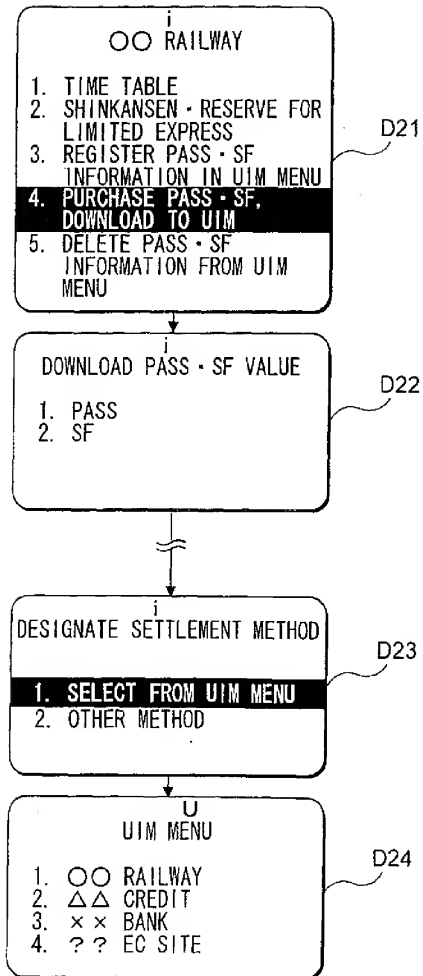


FIG. 17

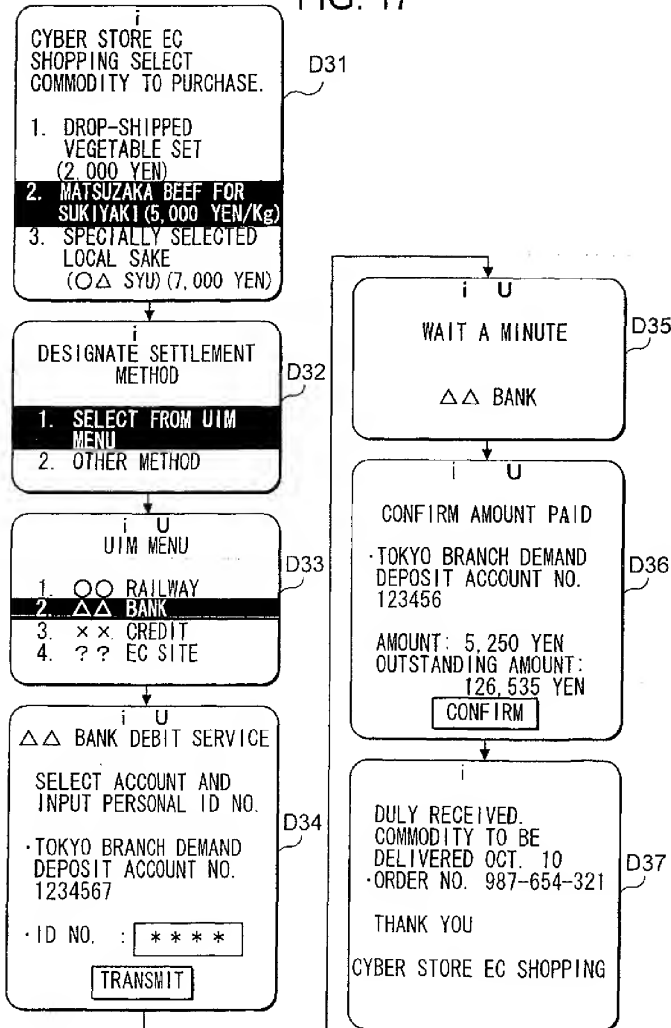


FIG. 18

(PRESS BUTTON TO UIM MENU)

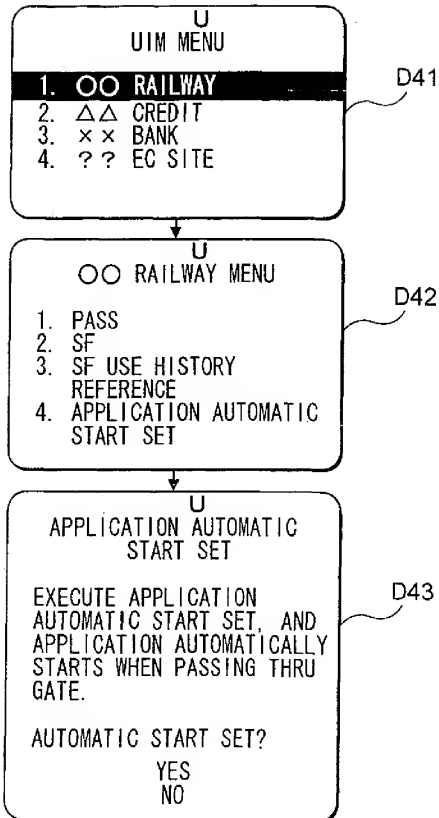


FIG. 19

(PRESS U BUTTON TO UIM MENU)

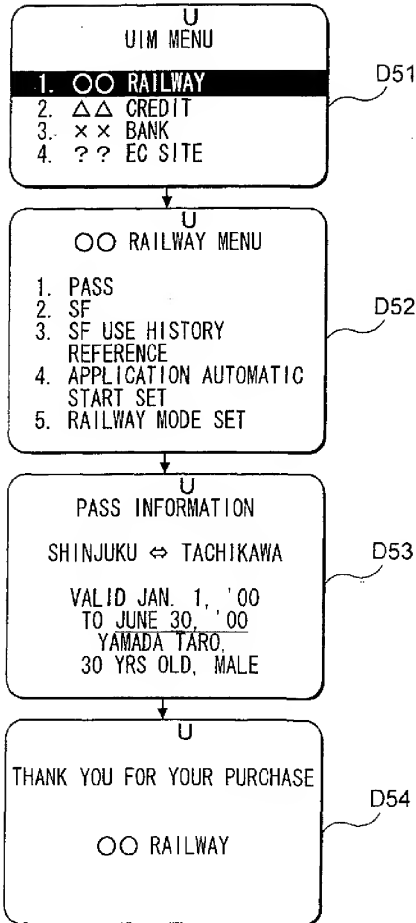


FIG. 20

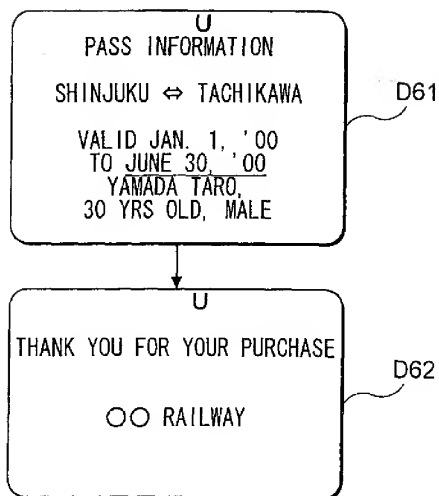


FIG. 21

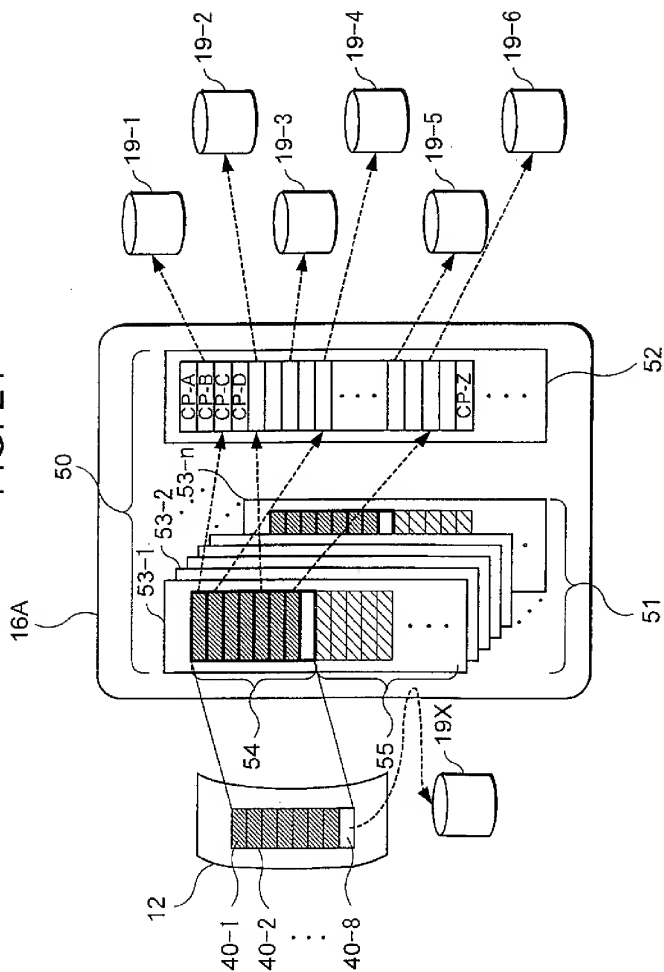


FIG. 22

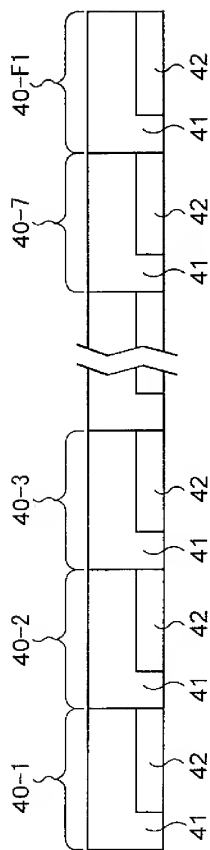
12C

FIG. 23

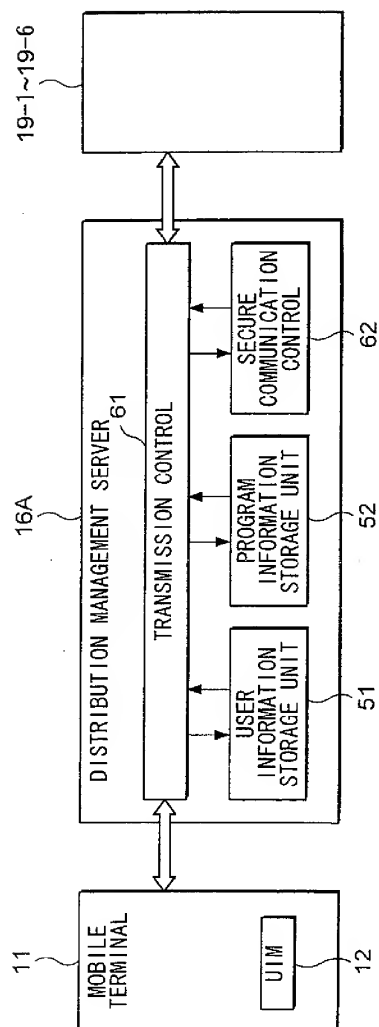


FIG. 24

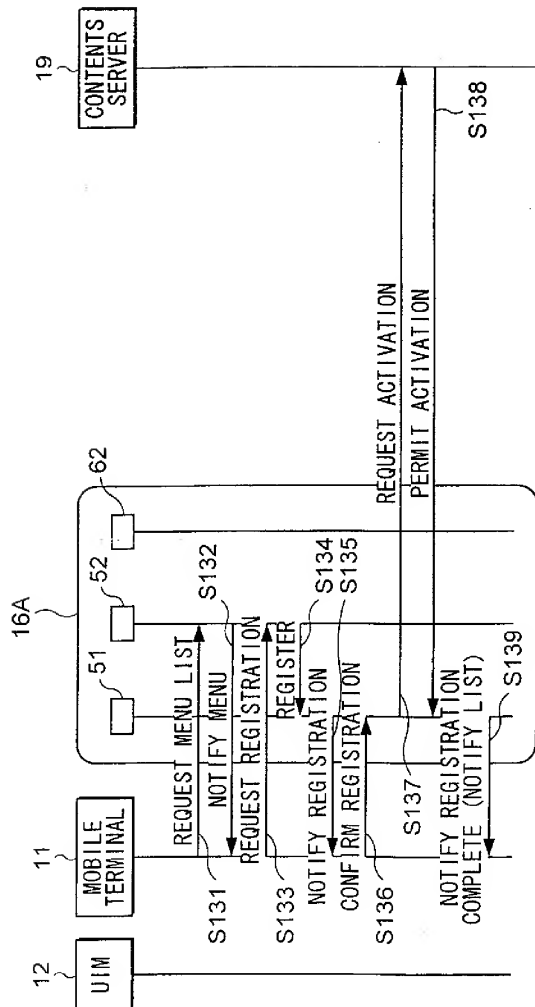


FIG. 25

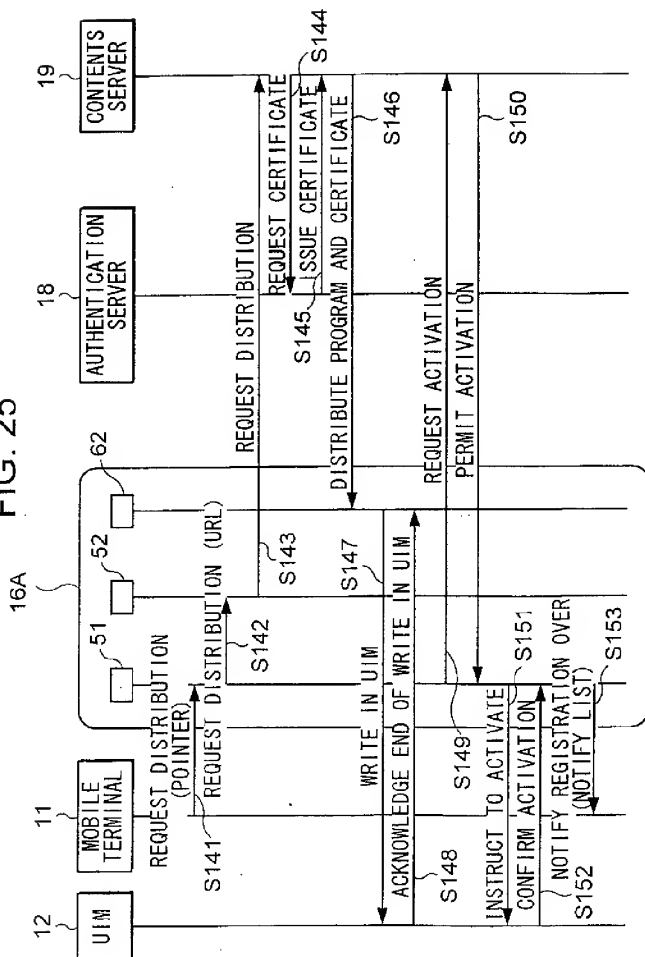


FIG. 26

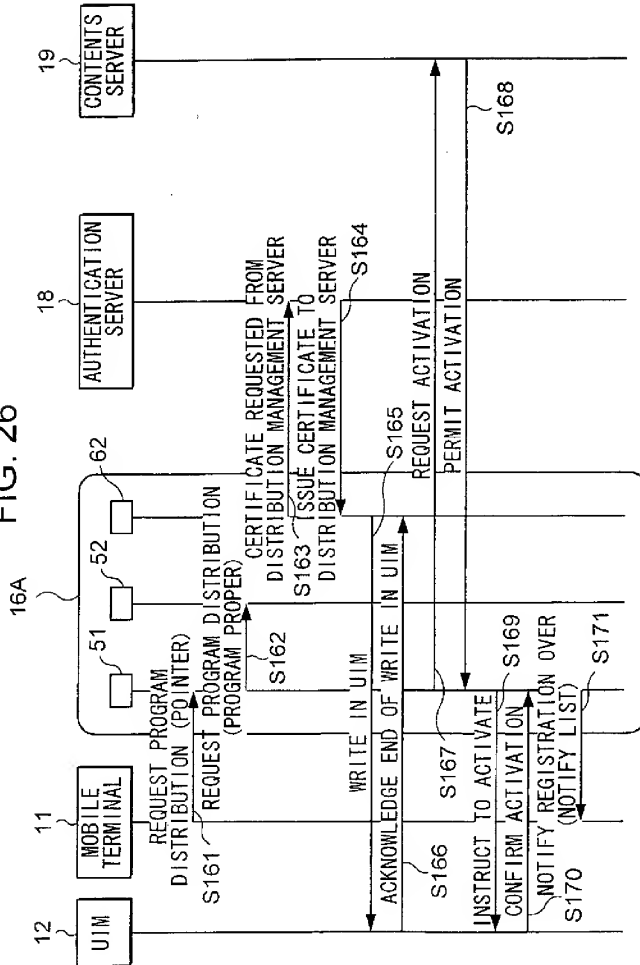


FIG. 27

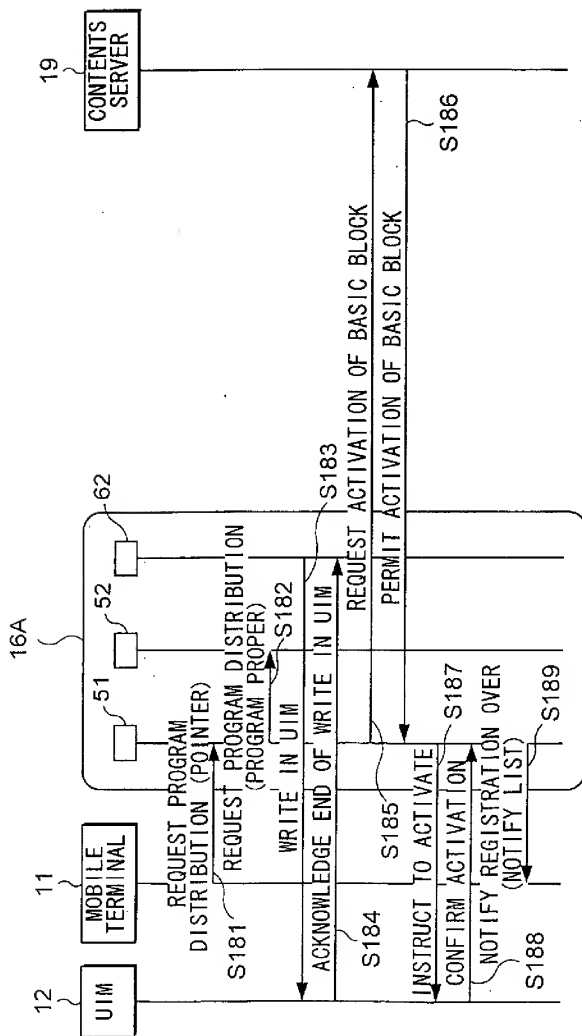


FIG. 28

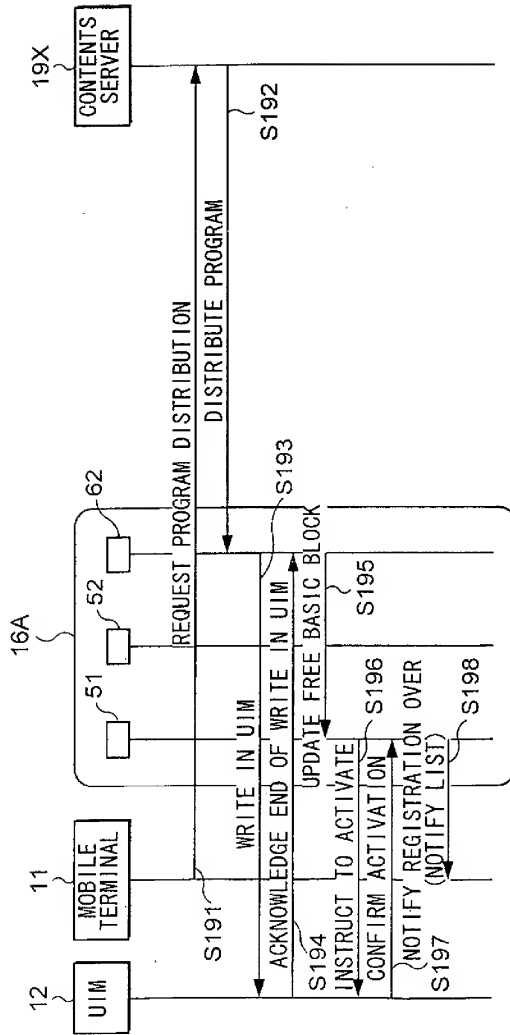


FIG. 29

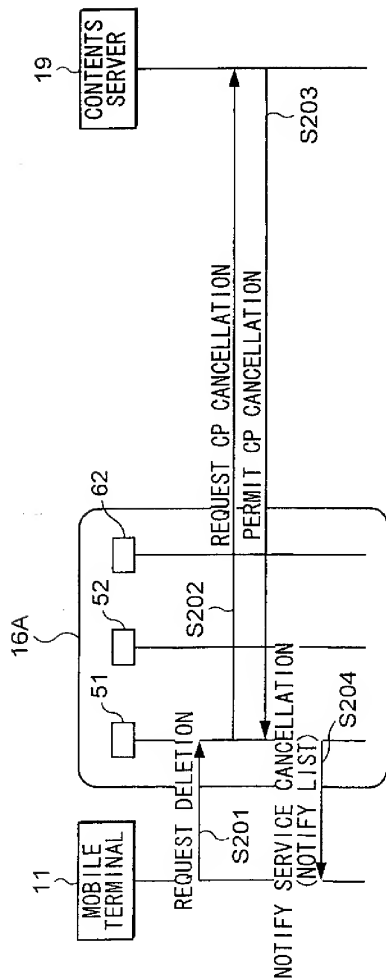


FIG. 30

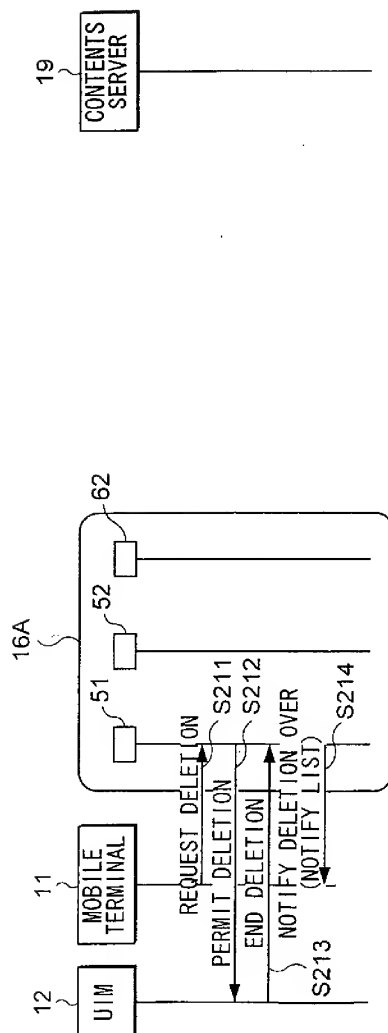


FIG. 31

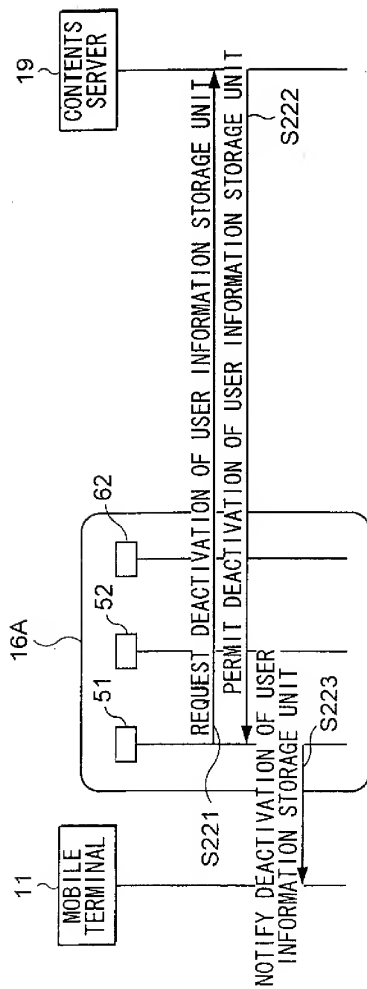
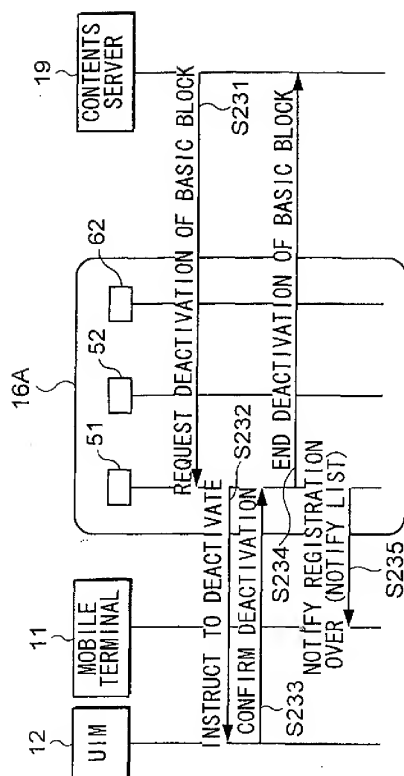


FIG. 32



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/00699

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.⁷ G06F9/06, G06F9/445

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ G06F9/06, G06F9/445

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Jitsuyo Shinan Toroku Koho	1996-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Toroku Jitsuyo Shinan Koho	1994-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-28786 A (San'yo Electric Co., Ltd.), 30 January, 2001 (30.01.01), Full text; Figs. 1 to 13 (Family: none)	1, 3-20, 22, 24-26, 28, 29, 31, 36, 37, 39 2, 21, 23, 27, 30, 32-35, 38
A		
Y	JP 2000-293584 A (Chugoku Nihon Denki Software Kabushiki Kaisha), 20 October, 2000 (20.10.00), Full text; Figs. 1 to 6 (Family: none)	1, 3-20, 22, 24-26, 28, 29, 31, 36, 37, 39
Y	JP 10-78867 A (Hitachi, Ltd.), 24 March, 1998 (24.03.98), Full text; Figs. 1 to 19 (Family: none)	4-7, 11, 12

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"I" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"P" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"Z" document: member of the same patent familyDate of the actual completion of the international search
08 May, 2002 (08.05.02)Date of mailing of the international search report
21 May, 2002 (21.05.02)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/00699

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 6-195217 A (Nippon Telegraph And Telephone Corp.), 15 July, 1994 (15.07.94), Full text; Fig. 1 (Family: none)	8, 9, 25

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

JP9135478A FM MULTIPLEX SIGNAL RECEIVER

Bibliography

DWPI Title

FM multiplier signal receiver reconfigures received display unit data and outputs display data containing completion time of reception of corresponding display unit data based on which image is output by display unit

Original Title

FM MULTIPLEX SIGNAL RECEIVER

Assignee/Applicant

Standardized: **SANYO ELECTRIC CO**

Original: SANYO ELECTRIC CO LTD

Inventor

TACHIBANA HIROYUKI ; MATSUI TAKEHARU ; MITSUFUJI HIRONORI ; SATA MASAHIRO

Publication Date (Kind Code)

1997-05-20 (A)

Application Number / Date

JP1995293015A / 1995-11-10

Priority Number / Date / Country

JP1995293015A / 1995-11-10 / JP

Abstract

PROBLEM TO BE SOLVED: To display the time of reception end corresponding to the contents of completely received page data concerning program data to be transmitted by FM multiplex broadcasting.

SOLUTION: The FM multiplex signal received by an antenna 12 and FM demodulated by an FM tuner part 14 is inputted to an FM multiplex decode part 15 and a base band signal is extracted. Based on the extracted base band signal, a CPU 40 at a personal computer 120 reconstitutes the program data. In that case, each time the page data are completely received, the time of reception end is possessed from a timer 50 and the contents of page data and the time of reception end are correspondently stored in a memory part 44. The CPU 40 correspondently displays the page data and the reception end time onto a display part 42.

【特許請求の範囲】

【請求項1】 伝送される複数の情報データの各々が複数の表示単位データに分割されて送信されるFM多重通信系において、前記各表示単位データと、対応する情報データ中の位置を示す番号データを含む送信データを受信するFM多重信号受信装置であって、

FM多重送信により前記表示単位データを伝送する搬送波を受信してFM復調する復調手段と、

前記復調手段の出力を受けて、FM多重信号を抽出し、対応するデジタル信号として出力するFM多重信号デコード手段と、

前記FM多重信号デコード手段の出力を受けて、前記各情報データに対応する前記表示単位データの受信を検知し、前記表示単位データにより再構成したデータと、対応する表示単位データの受信完了時刻とを含む表示データを出力する情報再構成手段と、

前記情報再構成手段の出力を受けて、前記表示データに対応する画像を出力する表示手段とを備える、FM多重信号受信装置。

【請求項2】 前記各表示単位データは、前記対応する情報データへの所属を示す識別データを含み、

前記情報再構成手段は、時刻データを出力する計時手段と、

前記FM多重信号デコード手段の出力と前記計時手段の出力とを受けて、前記表示単位データごとの受信完了と、対応する受信完了時刻とを検知し、前記識別データと前記番号データに応じて、対応する情報データごとに、前記表示単位データを再構成したデータと、前記受信完了時刻とを出力する演算手段と、

前記演算手段の出力を受けて、前記情報データごとに、前記表示単位データと対応する受信完了時刻を記憶する記憶手段とを含み、

前記演算手段は、前記記憶手段から、所定の数の前記表示単位データと対応する受信完了時刻を受け、対応する前記表示データを出力する、請求項1記載のFM多重信号受信装置。

【請求項3】 前記情報再構成手段および前記表示手段は、パーソナルコンピュータに含まれ、

前記復調手段および前記FM多重デコード手段は、着脱可能なインタフェース部により、前記パーソナルコンピュータと接続される、請求項2記載のFM多重信号受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数の表示単位データ（ページデータ）に分割されて送信される情報データを受信して、所定の数の表示単位データを出力する機能を有するデジタル信号受信装置に関し、特に、上記受信データがFM多重放送により伝送されるFM多重信号受信装置に関する。

【0002】

【従来の技術】近年、新しいサービスを提供する放送の1つとして、FMステレオ放送のベースバンド信号の空いたスペクトル領域に、デジタル信号を多重して送信するFM多重放送の開発・実用化が進められている。

【0003】FM多重放送は、現行FMステレオ放送の音声信号よりも高い周波数帯に新たにデジタル信号を多重し、交通情報、文字・図形情報などを放送する新しいメディアである。周波数を有効に利用できること、放送設備が簡易に実現できること、移動体でデータが受信できることから自動車等の移動体へ交通情報等を容易に伝送できることなどが特徴として挙げられる。

【0004】したがって、FM多重放送は、受信機を搭載した自動車等に対してリアルタイムでの渋滞情報等を伝送する手段として、あるいは、ハンディタイプの受信機を持つユーザに対して必要な情報をいつでもどこでもアクセスできる低廉な伝送路を提供する手段として、一部実用化が開始されている。

【0005】以下、従来のFM多重放送受信装置の構成について説明する前に、まずFM多重放送におけるデータ構造の概略を説明する。

【0006】[FM多重放送の方式] FM多重放送においては、受信状態を劣化させる要因として、マルチパス妨害やフェージング妨害がある。特に、移動体受信の場合においては、一般にその伝送路特性は非常に劣悪である。その場合でも、できるだけ一度で完全に受信できるシステムが望ましい。しかし、実際には、一度の受信で送信されたデータを完全に受信できない場合があり、その際には再送信されるデータを受信して、受信できなかったデータを補充することが前提となる。FM多重放送のサービスエリアは、FMステレオ放送のサービスエリアと同等であることが望ましいが、このサービスエリア内においても平均ビット誤り率が 10^{-2} を超えるような場所がある。したがって、送信されるデータの構造は、このような劣悪な伝送路特性を考慮して、その誤り訂正方式およびフレーム構成が決定されている。

【0007】特に、フェージング妨害による極端な電圧低下によって生ずる誤りは致命的であり、誤り訂正が不可能な場合がある。そこで、フェージングによって生ずる誤りの平均的なバースト長に送信されるデータの単位データ長を合わせることで、誤り訂正が不可能な誤りが生じた場合には、上記単位データごと再送信された単位データと置換えることで補充することが可能となる。

【0008】さらに、誤り訂正効果が高いことから、誤り訂正方式としては2つのブロック符号を直交して配置した積符号が用いられる。したがって、データは、縦方向および横方向ともに誤り訂正符号を含む2次元的なフレーム構造をとることになる。

【0009】そして、送信データは上記1フレーム中のデータを基本単位とする階層構造を有するデータ構造と

なる。

【0010】以上に述べたこと具体例として、さらに、文献(Proc. of Vehicle Navigation & Information Systems Conference (1994) A4-2 pp.111 ~ 116)に開示されている、FM多重放送方式について説明する。

【0011】図8に、上記データの階層構造の仕様を示す。階層1においては、伝送路特性が指定されている。通常のFMステレオ放送信号であるL+R信号およびL-R信号に加えて、L-R信号より高周波側に、多重信号が重畳される。

【0012】この重畳方式は、多重信号から音声信号への妨害が音声変調度が小さいときに顕著となることを考慮して、L-R信号の変調度により多重信号のレベルをコントロールするLMSK (Level controlled Minimum Shift Keying)方式が採用されている。

【0013】階層2は、誤り訂正方式を含む、データのフレーム構成が規定されている。各フレームは、列方向に272ブロックからなり、先頭には16ビットのB1C (Block Identification Code)が付加され、このB1Cに基づいてフレーム同期およびブロック同期が行なわれる。列方向の272ブロックのうち、190ブロックはデータを伝送するパケットであり、82ブロックは列方向のパリティを伝送するパリティパケットである。各パケットは、行方向に176ビットの情報部、誤り訂正符号である14ビットのCRC (Cyclic Redundancy Code)および82ビットのパリティ部より構成される。

【0014】つまり、送信データはこの1フレームを基本単位として、この段階でまず誤り訂正が行なわれる。

【0015】階層3は、データパケットの構成を規定する。データパケットは、フレーム内の各行のうち、B1C、CRCおよびパリティを除いた176ビットからなる。

【0016】さらに、このデータパケットは、プリフィックスとデータブロックで構成される。プリフィックスには、データの内容を識別するための情報が含まれ、たとえば後に述べるどの番組内容にそのデータパケットが属するかを指定している。

【0017】階層4は、データグループの構成を規定している。データグループは1つまたは複数データブロックで構成されている。すなわち、データパケットにおけるプリフィックス内の情報をもとに、データパケット番号の順に、データパケット番号が「0」から、プリフィックス内の情報出力フラグの立っているデータブロックまで並べることで構成される。このデータグループにも、誤り訂正符号であるCRCが含まれ、送信データはこの階層においても誤り訂正が行なわれる。

【0018】1つのデータグループは、1表示単位、すなわち1ページのデータに対応している。

【0019】階層5は、FM多重放送により伝送される一まとりの情報データ、すなわち番組データの構成を

規定する。図9は、この番組データの構成を示している。文字、図形情報の番組は複数のデータグループから構成され、先頭のデータグループは番組管理データとして、番組番号、ページ総数など番組全体にかかわる符号化された情報からなる。また番組管理データに引続いて、ページデータが複数個あり、1ページごとのデータが符号化されている。

【0020】番組データおよびページデータは、データヘッド部とデータユニット群から構成される。データユニット群は、文字データ部やフォトグラフィック図形データ部など、各符号化ごとに分割された複数のデータユニットにより構成されている。

【0021】つまり、以上のようなデータ構造においては、受信側において番組データが一まとりの情報を示す一群のデータをなしている。たとえば、交通情報であれば、番組情報は特定の路線(高速道路等)の各ジャンクションでの混雑状況等を示し、天気予報であれば、特定の地域における天気予報情報等を示すことになる。

【0022】[従来のFM多重放送受信機10の構成]図10は、従来のFM多重放送受信機10の構成を示す概略ブロック図である。

【0023】アンテナ12およびチューナ14によって受信されたFM多重放送信号が、検波回路16で検波され、さらにバンドパスフィルタ18を経て、LMSK復調回路20に与えらる。LMSK復調回路20は、LMSK変調されているFM多重放送信号のデータ復調を行ない、FM多重信号を取出す。復調されたデータ信号は、同期再生回路22において、図8における階層2において説明したとおりB1Cに基づいてフレーム同期およびブロック同期が行なわれる。同期されたデータ信号は、誤り訂正回路24において、パリティ符号およびCRCに基づいて誤り訂正される。

【0024】したがって、この誤り訂正回路24からは、正常に受信され、または誤り訂正が施されたFM多重放送のパケットデータ(図8における階層3において示した構成を有する。)が出力される。

【0025】中央演算処理装置40(以下、CPUと呼ぶ。)は、入力されたパケットデータに対して、データブロックの抽出、データグループの再構成およびデータグループ段階での誤り訂正ならびに番組データへの再構成を行なった後、番組データを表示装置42に出力する。表示装置42は、入力された番組データを図形あるいは文字として出力する。

【0026】ここで、表示装置42としては、1ページ分の表示領域、すなわち248×60ドット(日本語表示で15.5文字×2.5行に相当)を有する液晶画面等が用いられる。

【0027】

【発明が解決しようとする課題】従来のFM多重放送受信装置10は、上記のような構成であったので、以下の

ような問題点があった。

【0028】すなわち、FM多重放送により送信される情報データ、すなわち番組データとしては、たとえば上述のとおり交通情報や天気予報情報等が含まれる。これらの情報は、順次新しい情報が得られるたびにその番組内容が更新される。

【0029】しかしながら、従来のFM多重放送受信装置10においては、現在表示中の番組データが、いつ受信されたものであるかをユーザは知ることができない。このため、ユーザは、現在得られている情報の新鮮さの度合について判断することができないという問題があった。

【0030】本発明は、上記の目的のような課題を解決するためになされたものであって、その目的は、FM多重放送において、所定のページ数のページデータを表示する場合に、表示中の番組データ中のページデータについてその受信時刻を対応させて出力する機能を有するFM多重放送受信装置を提供することである。

【0031】

【課題を解決するための手段】請求項1記載のFM多重信号受信装置は、伝送される複数の情報データの各々が複数の表示単位データに分割されて送信されるFM多重通信系において、各表示単位データは、対応する情報データ中の位置を示す番号データを含む送信データを受信するFM多重信号受信装置であって、FM多重送信により表示単位データを伝送する搬送波を受信してFM復調する復調手段と、復調手段の出力を受けて、FM多重信号を抽出し、対応するデジタル信号として出力するFM多重信号デコード手段と、FM多重信号デコード手段の出力を受けて、各情報データに対応する表示単位データの受信を検知し、表示単位データにより再構成したデータと、対応する表示単位データの受信完了時刻とを含む表示データを出力する情報再構成手段と、情報再構成手段の出力を受けて、表示データに対応する画像を出力する表示手段とを備える。

【0032】請求項2記載のFM多重信号受信装置は、請求項1記載のFM多重信号受信装置の構成に加えて、前記各表示単位データは、対応する情報データへの所属を示す識別データを含み、情報再構成手段は、時刻データを出力する計時手段と、FM多重信号デコード手段の出力と計時手段の出力とを受けて、表示単位データごとの受信完了と、対応する受信完了時刻とを検知し、識別データと番号データに応じて、対応する情報データごとに、表示単位データを再構成したデータと受信完了時刻とを出力する演算手段と、演算手段の出力を受けて、情報データごとに、表示単位データと時刻とを記憶し、識別データと番号データに応じて、対応する情報データごとに、表示単位データを再構成したデータと受信完了時刻とを受け、対応する表示データを出力する。

【0033】請求項3記載のFM多重信号受信装置は、

請求項2記載のFM多重信号受信装置の構成において、情報再構成手段、入力手段および表示手段はパーソナルコンピュータに含まれ、復調手段およびFM多重デコード手段は、着脱可能なインタフェース部によりパーソナルコンピュータと接続される。

【0034】

【発明の実施の形態】図1は、本発明の実施の形態のFM多重放送受信装置100の構成を示す概略ブロック図である。

【0035】FM多重放送受信装置100は、FM電波を受けるアンテナ12と、アンテナ12の出力を受けてFM復調するFMチューナ部14と、FMチューナ部14の出力を受けてFM多重信号の抽出と誤り訂正を行ない、対応するデジタル信号を出力するFM多重デコード部15と、デジタル信号を受けて、表示単位データ（ページデータ）を構成し、対応する文字等を表示するパーソナルコンピュータ120を含む。

【0036】図10に示した、従来のFM多重放送受信装置10の構成と異なる点は、FMチューナ部14においてFM復調された信号から、FM多重デコード部15においてFM多重信号を抽出し、パケットデータとして出力されるデジタル信号を、パーソナルコンピュータ120が受け、パケットデータを番組データに再構成して表示する構成とした点である。

【0037】すなわち、アンテナ12によって受信されたFM多重放送信号は、FMチューナ部14におけるFM復調回路2において、フェーズロックドループ回路4（以下、PLL回路と呼ぶ。）から出力される局部発振波により同期検波され、バッファ6を介して、FM多重デコード部15に出力される。

【0038】FM多重デコード部15は、バッファ回路8を介して、FM復調された信号を受け、バンドパスフィルタ18により所定の周波数領域の信号成分を取出した後、復調LSI20においてLMSK復調を行なってFM多重信号を抽出する。

【0039】CPU26は、復調LSI20の出力を受けて、受信データのブロック同期、誤り訂正等を行なってパケットデータとして出力する。このとき、誤り訂正不能なパケットデータが存在する場合は、このCPU26においてそのデータが削除され、表示に必要なデータのみが選別されて出力される。

【0040】RAM28は、CPU26からの出力を受けて、インタフェース30に対してデータを出力するためのバッファとして動作する。

【0041】アドレスデコーダ32は、CPU26が、パーソナルコンピュータ120をアクセスしたことを検知すると、インタフェース30からデータを出力させる。

【0042】コントローラ34は、通常においては、インタフェース30からの出力データを受けて、パーソナル

ルコンピュータ120に対してデータの出力を行なう。ただし、装置の立上げ時などにおいては、ROM36に記憶されているデータに基づいて、インタフェース間の初期設定を行なう。

【0043】パーソナルコンピュータ120は、インタフェース38を介して、FM多重デコード部15から出力されるパケットデータを受ける。CPU40は、インタフェース38からの出力データ、すなわちパケットデータを受けて、図8において示した階層構造に従って、データパケットからデータブロックを抽出し、データブロックからデータグループを再構成し、データグループに対して誤り訂正を行なう。さらに、CPU40は、データグループ中のデータグループデータからページデータに相当するデータヘッダおよびデータユニット群を抽出し、番組データを再構成する。

【0044】このとき、CPU40は、各ページデータについて、受信が完了するたびにパーソナルコンピュータ120中のタイマ50の出力を受けて、その受信完了時刻を検知する。同時に、CPU40は、メモリ44に受信が完了した各ページデータと対応する受信完了時刻を、各番組データごとに記憶させる。さらに、CPU40は、各ページデータについて受信が完了しているか否かおよび各番組データについてその内容の更新が行なわれているか否かを常時モニタする。

【0045】以上のように再構成したページデータに基づいて、CPU40は、所定のページ数のページデータと対応する受信時刻とを選択して、表示部42に出力し、表示部42は、受取ったページデータに基づいて、対応する文字情報あるいは図形情報を出力する。

【0046】ここで、表示部42は、たとえばハンドヘルド型のパーソナルコンピュータでは、液晶フラットパネルディスプレイ等が用いられ、その表示領域は、640×400ドットあるいはそれ以上の解像度を持つ。

【0047】以下、図1のFM多重放送受信装置100の動作、特に、CPU40の動作について説明する。

【0048】FM多重放送受信装置100中のパーソナルコンピュータ120におけるCPU40の動作を説明する前に、その前提となるFM多重放送信号のデータ構造について、予め詳しく説明する。

【0049】図2は、図9に示した番組管理データを含むデータグループの構成を示す模式図である。図2に示したデータグループの構成のうち、データグループデータ中に番組管理データが含まれている。データグループは、その先頭にデータグループの開始を示すヘディング開始符号(SOH)を含み、それに続いて、データグループの連結の有無を示すフラグであるデータグループリンク符号と、データグループデータのバイト数を示すデータグループサイズデータを含む。それに引続いて、伝送されるデータの本体であるデータグループデータが存在する。さらにそれに続いて、データブロックの整数

倍の長さにデータグループ長を調整するための長さ調整用のNULL領域、データグループの終了を示す終了符号、データグループの誤り検出を行なうためのCRC符号が存在する。

【0050】図3は、図9に示した番組データのうち先頭の番組管理データに相当するデータグループの構造をさらに詳しく示した模式図の1例である。

【0051】図2において説明したとおり、先頭のデータブロックDB1にヘディング開始符号(SOH)が存在し、それに続くデータブロックDB2およびDB3にデータグループリンク符号(DGL)およびデータグループサイズのデータが存在する。データグループリンク符号およびデータグループサイズはデータグループヘッダと呼ばれる。その後、情報分離符号(RS)およびデータヘッダパラメータが続き、データブロックDB6から番組管理データ中の番組データヘッダの実質的な内容が開始する。番組データヘッダには、番組番号や、番組内容の更新が行なわれたことを示す更新データ、その番組中に含まれるページ総数、その番組の表示フォーマット等を指定する表示フォーマットデータが含まれている。番組管理データ中の番組データヘッダの後には、文字や図形データを含むデータユニット群が続いている。

【0052】一方、番組管理データに続く各ページデータにおいては、先頭にページデータヘッダが存在し、番組番号、そのページの番組中におけるページ番号や表示フォーマット等のデータを含んでいる。ページデータにおいても、ページデータヘッダの後に文字図形データを含むデータユニット群が続いている。

【0053】したがって、各ページデータに対応するデータグループごとに、そのページのページ番号に関するデータが含まれる構成となっている。

【0054】図4は、CPU40の動作のうち、ページデータの受信時刻を取得するサブルーチンの一例を示すフローチャートである。

【0055】CPU40は、FM多重デコード部15からの出力を受けて、ページデータの再構成を行ない、受信が完了したページデータが存在するか否かを常時モニタしている。同時に、CPU40は、番組管理データヘッダ内の更新データに基づいて、番組内容の更新が行なわれたか否かのモニタも行なっている。

【0056】現在受信中の番組データのいずれかのページデータの受信完了が検知されるか、あるいは番組内容の更新が検知された後の最初の1頁のページデータの受信が完了したことが検知されると、CPU40は、割込信号を発生し、受信時刻記憶ルーチンを開始する(ステップS11)。

【0057】CPU40は、タイマ50の出力を受けて、対応するページデータの受信完了時刻を取得する(ステップS12)。

【0058】CPU40は、続いて、受信完了時刻デー

タと受信が完了したページデータとをメモリ４４に対応させて記憶させる（ステップＳ１３）。

【００５９】以上の動作が終了すると受信時刻記憶ルーチンの動作が終了する（ステップＳ１４）。

【００６０】図５は、以上の動作により、メモリ４４内に記憶されている番組データを示す概念図である。メモリ４４には、各番組データごとに受信が完了したページデータの内容と、それに対応するページ番号および受信が完了した時刻がテーブルとして記憶されている。ＣＰＵ４０は、指定された表示開始ページから、順次受信が完了しているページデータの内容と受信完了時刻を読取することで、所定のページ数を表示部４２に表示させることが可能である。

【００６１】なお、図５は、ページ番号、ページデータの内容および受信完了時刻を記憶する概念を示したものであって、このようなテーブルをメモリ領域にどのように記憶させるかは、ソフトウェアやハードウェアの構成に依りて変化する。

【００６２】図６は、表示部４２にページデータを表示させる表示画面の一例を示す模式図である。

【００６３】表示領域３５０には、受信した番組データのうちの指定されたページデータが表示され、表示領域３５２には、対応するページ番号が表示される。

【００６４】表示領域３７０には、現在表示中のページデータに対応する受信完了時刻が表示されている。

【００６５】なお、図６に示した模式図においては、１頁分のデータを表示する場合について示したが、ページめくりボタン（＋）３６２等をユーザが選択することにより、表示領域３５０の大きさを変化させて、複数頁を同時に出力する構成とすることも可能である。

【００６６】この場合、ページデータに対応する受信時刻の表示も、たとえば、表示中の最初のページデータに対応した受信時刻を表示する構成や、表示中のすべてのページデータについての受信時刻を表示する構成とすることも可能である。

【００６７】以上のような構成とすることで、メモリ４４には、受信が完了したページデータの内容とそれに対応する受信完了時刻が記憶され、表示部４２に両者が対応して表示されるので、ユーザは常に表示中のページデータの新鮮さの度合を知ることが可能である。しかも、番組内容が更新されるごとに、このページデータの受信完了時刻も更新されるので、常に、最新の番組データについて、それに含まれるページデータの新鮮さの度合を判断することが可能となる。

【００６８】図７は、図１に示したＦＭ多重放送受信装置１００をノートブック型パソコン１２０とＩＣカードを用いて構成した場合の概略図を示す。

【００６９】この場合、ＦＭ多重デコード部１５がＩＣカード化され、パーソナルコンピュータ１２０に対して着脱可能となっている。ＦＭチューナ部１４は、ＦＭ多

重デコード部１５と接続コードによって接続される構成としている。以上のような構成とすることにより、ＦＭチューナ部１４をパーソナルコンピュータ１２０から遠ざけることが可能となり、受信信号にパーソナルコンピュータ１２０からのノイズが混入することを防止することが可能となる。

【００７０】もちろん、図７に示したようにＦＭチューナ部１４とＦＭ多重デコード部１５とを接続コードにより接続する構成ではなく、両者を一体化することで、より携帯に便利な形とすることも可能である。

【００７１】

【発明の効果】 上述のように、本発明によれば、ＦＭ多重放送を受信中のユーザは、表示中のページデータの受信完了時刻を知ることが可能で、現在受取っているデータの新鮮さの度合を把握することが可能である。

【図面の簡単な説明】

【図１】 本発明に係るＦＭ多重放送受信装置１００の構成を示す概略ブロック図である。

【図２】 ＦＭ多重放送信号におけるデータグループの構成を示す模式図である。

【図３】 ページデータにおけるページデータヘッダの構成を示す模式図である。

【図４】 本発明のＦＭ多重放送受信装置１００におけるＣＰＵ４０の動作を示すフローチャートである。

【図５】 メモリ４４の記憶状態の一例を示す概念図である。

【図６】 表示部４２の表示例を示す模式図である。

【図７】 本発明に係るＦＭ多重放送受信装置の外観を示す模式図である。

【図８】 ＦＭ多重放送の仕様の示す仕様図である。

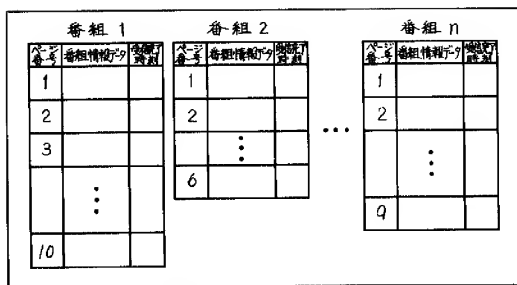
【図９】 番組データの構成を示す模式図である。

【図１０】 従来のＦＭ多重放送受信装置１０の構成を示す概略ブロック図である。

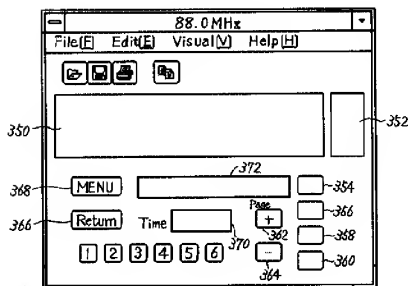
【符号の説明】

- ２ ＦＭ復調回路
- ４ ＰＬＬ回路
- ６、８ バッパ回路
- １０ 従来のＦＭ多重放送受信装置
- １２ アンテナ
- １４ チューナ
- １６ 検波回路
- １８ バイパスフィルタ
- ２０ ＮＭＳＫ復調回路
- ２２ 同期再生回路
- ２４ 誤り訂正回路
- ２６ ＣＰＵ
- ２８ ＲＡＭ
- ３０、３８ インタフェース回路
- ３２ アドレスデコーダ
- ３４ コントローラ

【図5】

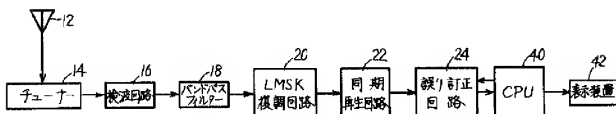


【図6】



【図10】

10



フロントページの続き

(72)発明者 佐多 正博

大阪府守口市京阪本通2丁目5番5号 三
洋電機株式会社内

JP11243569A

MESSAGE RECEIVER

Publication number : JP11243569A

Date of publication of application : 07.09.1999

Application number : 10-060468

Applicant : KOKUSAI ELECTRIC CO LTD

Date of filing : 25.02.1998

Inventor : TAMAKUMA YUUCHI

Abstract:

PROBLEM TO BE SOLVED: To select received information message according to a specific code set for each message receiver so as to store it in a storing means.

SOLUTION: This message receiver radio-receives an individual selective calling number and a group calling number, and when the received individual selective calling number and group calling number are coincident with a calling number assigned to itself, stores the received message in a storing means 65 corresponding to the calling number and displays it on a display 67. Then in order to select an information message concerning group calling, a specific code regulating the storing propriety of information message in the storing means 79 has been stored previously in a specific code storing means 78, and when a specific code added to the radio-received information message is coincident with the specific code, the information message is stored in the means 79. Thereby, according to the setting of the specific code obtained furthermore by subdividing the group calling number, the information message is prevented from being stored in order to prevent the wasteful consumption of a memory capacity.

【特許請求の範囲】

【請求項1】 メッセージ受信機に共通な情報メッセージを提供するための群呼出番号を無線受信すると、自己に割り当てられている群呼出番号に対応する情報メッセージを記憶手段に格納するメッセージ受信機において、特定コードを保持する特定コード記憶手段と、群呼出番号に対応して受信した情報メッセージに付加されている特定コードと前記特定コード記憶手段に保持されている特定コードとを比較する比較手段と、前記比較によって両特定コードが一致している場合に当該特定コードが付加された情報メッセージを前記記憶手段に格納する格納手段と、を備えたことを特徴とするメッセージ受信機。

【請求項2】 請求項1に記載のメッセージ受信機において、前記特定コードを受け付ける入力手段を更に有し、前記特定コード記憶手段は前記入力手段から受け付けた特定コードを書き換え可能に保持することを特徴とするメッセージ受信機。

【請求項3】 請求項1又は請求項2に記載のメッセージ受信機において、前記記憶手段に格納される情報メッセージを表示出力するメッセージ表示手段を有することを特徴とするメッセージ受信機。

【請求項4】 個別選択呼出番号と群呼出番号とを無線受信して、受信した個別選択呼出番号或いは群呼出番号が自己に割り当てられた呼出番号と一致した場合に、当該個別選択呼出番号あるいは当該群呼出番号に対応して受信したメッセージを記憶手段に格納し、表示器に表示する携帯可能なメッセージ受信機において、前記記憶手段は、個別選択呼出番号に対応して受信したメッセージを記憶するメッセージ格納エリアと、群呼出番号に対応して受信した情報メッセージを記憶する受信情報格納エリアとに分割されており、更に、メッセージ受信機に共通な情報メッセージを提供するための群呼出番号及び情報メッセージ及び特定コードを含む無線信号を受信する受信手段と、自己に割り当てられた群呼出番号を記憶する呼出番号記憶手段と、受信した情報メッセージの格納の可否を規定する特定コードを記憶する特定コード記憶手段と、前記受信手段で受信した群呼出番号と前記呼出番号記憶手段に記憶された自己の群呼出番号との一致を判定する呼出番号比較手段と、前記受信した群呼出番号と自己の呼出番号とが一致した場合に、受信信号から特定コードを抽出する特定コード抽出手段と、前記特定コード記憶手段に記憶された特定コードと前記抽出された特定コードとの一致を判定する特定コード比較手段と、

前記受信した特定コードと自己の特定コードとが一致した場合に、前記受信信号から情報メッセージを抽出して当該情報メッセージとを前記記憶手段の受信情報格納エリアに記憶させる格納手段と、を備えたことを特徴とするメッセージ受信機。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、自己宛のメッセージを無線受信して記憶格納するメッセージ受信機に関し、特に、受信したメッセージを各メッセージ受信機毎に設定した特定コードに応じて記憶手段に格納しないようにしたメッセージ受信機に関する。

【0002】

【従来の技術】近年、ページ等のメッセージ受信機を用いた無線選択呼出通信システムは、数字情報のみならず平仮名や漢字等の文字情報をも送信可能になり、単に個人宛てにメッセージを送るだけでなく、情報提供会社が提供するニュース、株価、天気等の各種情報をも送信可能となっている。このような無線選択呼出通信システムにおいて、上記提供された天気情報等は共通の呼出番号（群呼出番号）宛てに無線送信され、この群呼出番号をもつ複数のメッセージ受信機が上記情報を受信して表示する情報提供サービスが行われている。

【0003】このような情報提供サービスを行うために、例えば特公平5-35933号公報には、2つのコードのうちの1つを個別選択呼出サービスに使用し、他の1つを情報提供サービスに使用する発明が開示されている。しかしながら、この発明にあつては、受信したメッセージがサービス情報に係る情報メッセージであれば、その呼出番号が一致すれば、メモリに記憶するようになっていた。

【0004】

【発明が解決しようとする課題】ここで、上記のようなサービス情報に係る情報メッセージは個別メッセージに比して多種多様に頻りに送信されるが、実際の使用状況を調査してみると、送信されてくる情報メッセージの内の全ての種類を常に利用者が必要とするわけではなく、個々の利用者或いは時や場合に応じて、必要とする情報メッセージの種類が異なるものである。しかしながら、従来のメッセージ受信機にあつては、自己宛の群呼出番号が一致している限り、これら全ての情報メッセージを受信してメモリに記憶格納することとなるため、利用者が必要としない情報メッセージまでも記憶格納して、必要なメッセージを記憶するためのメモリ容量が減少してしまうという問題があつた。

【0005】また、従来のメッセージ受信機にあつては、同一の群呼出番号を有する情報メッセージの内で情報メッセージの種類に応じて、利用者を受信許可を設定することができず、多くの利用者の個々に対して情報メッセージの配給状態を細かく設定することができないと

いう問題があった。また、従来のメッセージ受信機であっても、情報提供会社からの各種サービス情報を受信しても、当該サービス情報（情報メッセージ）は個人宛ての通常の個別メッセージと同じメモリエリアに格納するため、個別メッセージを受信するためのメモリ容量が減少し、多くの情報メッセージを記憶保持してしまう場合にも、個別メッセージを受信しても記憶表示させることができない事態も生じてしまうという問題もあった。

【0006】本発明は上記従来の事情に鑑みなされたもので、情報メッセージを更に特定コードに基づいて管理し、情報メッセージはその特定コードによって記憶格納しないようにして、メモリ容量を有効に活用することができるとする。なお、本発明の更なる具体的な目的は、以下の説明において記載するところである。

【0007】

【課題を解決するための手段】本発明に係るメッセージ受信機は、例えばページャにおいて実施され、個別選択呼出番号と少なくとも1つの群呼出番号とを無線受信して、受信した個別選択呼出番号あるいは群呼出番号が自己に割り当てられた呼出番号と一致した場合に、当該個別選択呼出番号あるいは当該群呼出番号に対応して受信したメッセージを記憶手段に格納するとともに表示器に表示する。そして、本発明では特に、共通情報提供サービスの群呼出に係る情報メッセージを取捨選択するために、情報メッセージの記憶手段への格納可否を規定する特定コードを予め特定コード記憶手段に記憶保持しており、群呼出番号に対応して無線受信した情報メッセージに付加されている特定コードが記憶格納されている特定コードに一致した場合に、当該情報メッセージを記憶手段に格納するようにしている。これにより、群呼出番号を更に細分化した特定コードの設定に応じて、情報メッセージを記憶格納しないようにして、メモリ容量の無駄な消費を防止する。

【0008】また、本発明に係るメッセージ受信機では、当該受信機の供給元による設定以外に、情報メッセージを取捨選択するために、利用者が任意に入力する特定コードを入力手段から受け付けて、当該特定コードを書き換え可能に特定コード記憶手段に保持する。これにより、利用者が不要とする種類の情報メッセージは、特定コードの設定に応じて記憶格納しないようにして、メモリ容量の無駄な消費を防止する。

【0009】また、本発明に係るメッセージ受信機は、メッセージの受信格納機能だけを有した装置として構成し、受信した情報メッセージを別個な表示装置で表示出力するようにしてもよいが、記憶手段に格納される情報メッセージを表示出力するメッセージ表示手段を有して構成すれば、受信したメッセージを利用者が手軽に表示出力させることができる。

【0010】本発明は、好ましい態様として、個別選択

呼出番号と群呼出番号とを無線受信して、受信した個別選択呼出番号あるいは群呼出番号が自己に割り当てられた呼出番号と一致した場合に、当該個別選択呼出番号あるいは当該群呼出番号に対応して受信したメッセージを記憶手段に群呼し、表示器に表示する携帯可能なページャ等のメッセージ受信機として実施され、記憶手段は、個別選択呼出番号に対応して受信したメッセージを記憶するメッセージ格納エリアと、群呼出番号に対応して受信した情報メッセージを記憶する受信情報格納エリアとに分割されている。そして、受信手段で、群呼出番号及び情報メッセージ及び特定コードを含む無線信号を受信すると、受信した群呼出番号と呼出番号記憶手段が記憶する自己の群呼出番号とを呼出番号比較手段が比較し、この結果、両者が一致した場合に、特定コード抽出手段が受信信号から特定コードを抽出する。そして、特定コード記憶手段に記憶された特定コードと抽出された特定コードが一致しているかを特定コード比較手段が判断し、この結果、両者が一致している場合のみ、格納手段が受信信号に含まれている情報メッセージを記憶手段の受信情報格納エリアに記憶させる。これにより、個別選択呼出に係るメッセージの格納容量を確保し、更に、群呼出に係るメッセージの格納容量を有効活用し、個別選択呼出と群呼出とに支障のないように記憶手段の限られたメモリ容量を活用する。

【0011】

【発明の実施の形態】本発明を、メッセージ受信機（あるいは、表示機能付選択呼出受信機）としてページャを用いた無線選択呼出通信システムの一実施形態を用いて詳しく説明する。本例の無線選択呼出通信システムは、図1に示すように、情報提供会社1、電話機2、電話網3、中央局4、基地局5A、5B、・・・、5N、ページャ6A、6B、・・・、6Nで構成されている。このシステム構成において、情報提供会社1が作成した情報メッセージまたは電話機2あるいは別の入力装置（図示せず、例えば、携帯電話、パーソナルコンピュータ等）からの個別呼出のための通常の個別メッセージが電話網3を介して中央局4に送信される。

【0012】中央局4は上記の情報メッセージや個別メッセージの送信相手の呼出番号及びメッセージ信号を無線通信システムに適したプロトコルに変換して複数の基地局5A～5Nへ送信する。なお、無線通信システムに適したプロトコルとしては、例えば、POCSAG (Post Office Code Standardization Advisory Group)、NTT方式、RCR STD-42Aに規定されているFLEX-RTD RADIO PAGING SYSTEM (以下FLEX-RTDとする)等のプロトコルがあるが、本発明は他の形式も利用することができる。

【0013】基地局5A～5Nは上記のように変換されたデータ予め決められたデータ伝送速度（例えば、FLEX-RTDでは、1、600bps（ビット毎秒））、

3, 200bps或いは6, 400bps)の無線信号で複数のページ6A~6Nに送信する。ページ6A~6Nは上記の無線信号を受信して、この無線信号中に自己に割り当てられた呼出番号と一致する信号を検出したときに、呼出報知及び受信したメッセージ内容の表示を行う。

【0014】次に、図2を用いて基地局5A~5Nから送信される無線信号のフレームフォーマットの一例を説明する。同図に示すように、送信フレームフォーマットは、同期部20、ブロック情報(BI)21、アドレスフィールド(AF)22、ベクトルフィールド(VF)23、メッセージフィールド(MF)24で構成される。同期部20は、「1」と「0」とのパターンで構成され、ページ6A~6Nに対して同期のタイミングを与える信号である。ブロック情報21は、フレーム及びシステム構成の情報を含み、アドレスフィールド22の起点、ベクトルフィールド23の起点、トラフィックが次のフレームへ続くことを示す情報等からなるフィールドである。アドレスフィールド22は、特定のページを呼び出す個別呼出番号または情報提供会社1からの情報を共通して受信することができるページを特定するための群呼出番号が1つ以上格納されるフィールドである。

【0015】また、ベクトルフィールド23は、上記の個別呼出番号或いは群呼出番号に対応する個別メッセージ或いは情報メッセージが次に続くメッセージフィールド24のどの位置に格納されているかの情報、そのメッセージ内容の長さを示す情報、メッセージ内容が文字、メッセージ内容が英数字、メッセージ内容が16進/2進であることを示す等のメッセージのタイプを示す情報等が格納されるフィールドである。メッセージフィールド24は、個別呼出番号或いは群呼出番号に対応する個別メッセージ或いは情報メッセージが格納されるフィールドである。

【0016】次に、ページに情報提供会社1からの共通情報を提供するための群呼出番号がアドレスフィールド22に格納された場合の、メッセージフィールド24のフォーマットの一例を図3を用いて説明する。図3に示すように、メッセージフィールド24は、特定コード241、情報メッセージ本文フィールド242で構成される。特定コード241は情報メッセージ本文フィールド242の内容により特定される番号が挿入され、例えば数桁の数字とこの数桁の数字が特定コードであることを示す記号とが挿入される。情報メッセージ本文フィールド242には情報提供会社1等が作成した情報メッセージ本文(文字等で記述されたメッセージの内容)が挿入される。なお、本例では、各情報メッセージにはその種類を表示するためのタイトル情報が付加されており、このタイトル情報は情報メッセージと共に情報メッセージ本文フィールド242に挿入されている。

【0017】図4は、本例のページの実施例を示すブロック図である。本例におけるページ6A~6Nにおいて、60は無線信号を受信するアンテナ、61は基地局5A~5Nから送信された上記如きのフレームフォーマットの無線信号をアンテナ60を介して受信する受信部、62は受信した信号を復号するデコーダ部、63は予め割り当てられた自己の個別選択呼出番号及び情報メッセージを受信するために割り当てられた群呼出番号及び受信すべきフレームの番号を記憶するID-ROM、64は各機能部を制御するための各種プログラムが格納されているROM、65は特定コード及び受信したメッセージを格納するためのRAM、66は制御部72からの入力信号に基づいて表示部67を駆動する表示駆動回路、67はメッセージ等を表示するLCD等の表示部、68は呼出があったことを光により報知するためのLED、69は呼出があったことを音により報知するためのスピーカ等の鳴音部、70は呼出があったことを振動により報知するためのバイブレータ等の振動部、71はメッセージの読み出しや呼出動作の停止及び文字や数字の入力、特定コードの入力等を利用者が行うための操作部である。

【0018】ここで、本例の通信システムは、メッセージ等のデータを複数のフレームで重複して送信するダイバーシチ的な形式としていることから、ID-ROM63には受信すべきフレームの番号が記憶されて、当該フレームの番号に基づいて各ページ6A~6Nは自己に該当するフレームを受信処理する。なお、本発明はこのような形式の通信システムに限らず、他の種々な形式の通信システムにおいても実現できることは勿論である。

【0019】また、このページには上記の各機能部61~71を統括制御する制御部72が備えられており、この制御部72は、受信した信号のアドレスとID-ROM63に記憶されている個別呼出番号或いは群呼出番号との比較を行うID比較手段73と、受信した信号が群呼出番号と一致した場合に次に続く情報メッセージの特定コードを抽出する特定コード抽出手段74と、この抽出手段74により抽出された特定コードとRAM65の特定コード記憶手段78に格納されている特定コードとを比較する特定コード比較手段75と、特定コードが一致した場合に次に続く情報メッセージを抽出する情報メッセージ抽出手段76と、受信した信号が個別呼出番号と一致した場合に次に続く個別メッセージを抽出する通常メッセージ抽出手段77と、が備えられている。

【0020】更に、上記RAM65は、操作部71により入力された特定コードを書き換え可能に格納する特定コード記憶手段78と、群呼出番号及び特定コードが一致した場合の情報メッセージを書き換え可能に格納する受信情報格納エリア79と、個別呼出番号に一致した個別メッセージを書き換え可能に格納する通常メッセージ格納エリア80と、が形成されている。なお、本例で

は、同一のメモリフィールドに3つのエリアを分割して形成しているが、これらエリアを互いに異なるメモリ装置によって構成してもよい。また、情報メッセージ及び通常のメッセージを同一のメモリ内に格納するようにしてもよい。上記のように複数のエリアを分割するのが好ましいが、本発明の他の目的からすれば、このようにエリアを分割することは必須ではない。

【0021】図5には、図4に示した特定のコードを格納するための特定コード記憶手段（特定コード記憶エリア）78の構成を示してある。この特定コード記憶エリア78は、操作部77により入力された複数の特定コード及びこの特定コードに対応するタイトルが書き換え可能に格納され、例えば、番号“2”として特定コード“001”及びタイトル“日本の政治ニュース”が格納され、これによって、当該特定コード“001”を含んだ群呼出信号を受信したときに、当該信号に含まれる情報メッセージが受信情報格納エリア79に格納されるようになっている。ここで、本例では、情報メッセージにタイトル情報も含まれていることから、対応するタイトル情報も特定コード記憶手段78に格納するようにしたが、本発明においては、特定コードのみを特定コード記憶手段78に格納させるように構成してもよい。

【0022】図6には、情報メッセージを格納するための受信情報格納エリア79の構成を示してある。この情報メッセージ格納エリアには、群呼出番号及び特定コードが一致した場合に、一致した特定コードとこの特定コードが付加されて送信された情報メッセージ（メッセージ内容）とが受信順に書き換え可能に格納される。例えば、受信番号“3”として特定コード“002”が付加されて送信されてきた情報メッセージの内容“（スポーツ）に関するメッセージ”が格納され、受信時及び操作部71からの表示指示の入力時に、これら格納されたメッセージの内容は表示部67から表示出力される。なお、本例では、受信情報格納エリア79に受信信号から抽出した特定コードも格納するようにしているが、本発明においてはこの特定コードを格納することは必須ではない。

【0023】図7には、上記したページャにおける受信処理動作の一例を示してある。まず、受信部61がID-ROM63に記憶されている自己の呼出番号が含まれるフレームを受信すると（ステップS1）、受信したフレームのアドレスフィールド22の呼出番号とID-ROM63に記憶されている個別呼出番号との比較をID比較手段73で行い（ステップS2）、この比較の結果、両者が一致しない場合には後述するステップS7以降の処理を行う。一方、両者が一致した場合には、続くベクトルフィールド23を参照してメッセージがあるかどうかの判断を制御部72で行う（ステップS3）。そして、メッセージが存在する場合には、受信フレームからメッセージを通常メッセージ抽出手段77により抽出し

て、通常メッセージ格納エリア80に記憶するとともに（ステップS4）、表示駆動回路66を制御して表示部67に当該メッセージの表示を行い（ステップS5）、更に、LED68、鳴音部69或いは振動部70により呼出があったことの報知動作を行う（ステップS6）。なお、ステップS3でメッセージが存在しないときは、呼出があったことのみをLED、鳴音部或いは振動部に呼び報知する（ステップS6）。

【0024】上記したように受信呼出番号と自己の個別呼出番号とが一致しない場合には（ステップS2）、まず、受信呼出番号とID-ROM63に記憶されている群呼出番号との比較をID比較手段73が行い（ステップS7）、両者が一致しない場合には受信動作を終了する。一方、両者が一致した場合には、制御部72は次に続くベクトルフィールド23を参照して情報メッセージがあるかどうかの判断を行い（ステップS8）、情報メッセージが存在しない場合には受信動作を終了する。一方、情報メッセージが存在した場合には、特定コード抽出手段74が受信フレーム中に特定コード241が存在するかどうかを確認し（ステップS9）、特定コード241が存在しない場合には受信動作を終了する。

【0025】一方、特定コード241が存在する場合には、特定コード抽出手段74が当該特定コードを受信フレームから抽出し、この抽出した特定コードと予め特定コード記憶手段78に登録されている特定コードとを特定コード比較手段75が比較する（ステップS10）。この結果、両者が一致しない場合には、このページャにおいては群呼出番号は一致するが格納を許可された情報メッセージではないので、次に続く情報メッセージの抽出及びメモリへの格納を行わずに受信処理を終了する。一方、両者が一致した場合には、受信フレーム中の次に続く情報メッセージを情報メッセージ抽出手段76が抽出して受信情報格納エリア79に格納し、受信した情報メッセージの表示（ステップS5）及び呼出の報知を行う（ステップS6）。

【0026】なお、上記の説明では本発明をページャに適用した例を示したが、本発明はページャに限らず、情報を受信する機能を持つ、例えば、パーソナルコンピュータ、ラジオ受信機、携帯電話機等といった種々な形態で実施することもできる。

【0027】

【発明の効果】以上説明したように、本発明によると、利用者の要否等に応じて受信した情報メッセージをメモリに格納しないようにしたため、メモリ容量の浪費を使用状況に応じて効果的に抑えることができ、メモリ容量の有効活用を実現することができる。特に、個別呼出も併用するメッセージ受信機にあつては、個別呼出のメッセージを格納するためのメモリ容量が圧迫されず、個別メッセージと情報メッセージとの格納を限られたメモリ容量において支障なく実現することができる。また、サ

ービス情報が多様化するに伴って群呼出番号を多くしなければならないが、本発明によれば群呼出番号の増加を抑えることができ、例えば、1つの群呼出番号のみであっても、情報メッセージ内容により決められた特定コードを利用者がメッセージ受信機に登録しておくだけで、必要な情報メッセージだけを受信格納することができる。

【図面の簡単な説明】

【図1】 本発明の一実施形態に係る選択呼出通信システムの構成を示す図である。

【図2】 本発明の一実施形態に係る送出フレームの構成を説明する図である。

【図3】 本発明の一実施形態に係るメッセージフィールドの構成を説明する図である。

【図4】 本発明の一実施形態に係るページャの構成を示す図である。

【図5】 本発明の一実施形態に係る特定コード記憶エ

リアの構成を説明する図である。

【図6】 本発明の一実施形態に係る情報メッセージ格納エリアの構成を説明する図である。

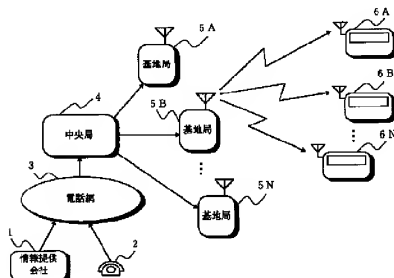
【図7】 本発明の一実施形態に係るページャの受信処理の一例を示すフローチャートである。

【符号の説明】

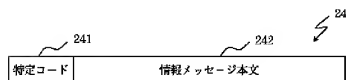
1・・・情報提供会社、 4・・・中央局、 5A～5N・・・基地局、 6A～6N・・・ページャ、 24・・・メッセージフィールド、 61・・・受信部、 63・・・ID-ROM、 65・・・RAM、 67・・・表示部、 71・・・操作部、 73・・・ID比較手段、 74・・・特定コード抽出手段、 75・・・特定コード比較手段、 76・・・情報メッセージ抽出手段、 77・・・通常メッセージ抽出手段、 78・・・特定コード記憶手段、 79・・・受信情報格納エリア、 80・・・通常メッセージ格納エリア、 241・・・特定コード、

【図1】

システム構成図

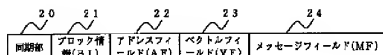


【図3】



【図2】

フレームフォーマット



【図5】

特定コード記憶手段

番号	特定コード	タイトル
1	0 0 0	日本の経済ニュース
2	0 0 1	日本の政治ニュース
3	0 2 2	スポーツ
4	0 5 0	天気
.	.	.
.	.	.
N-1		
N		

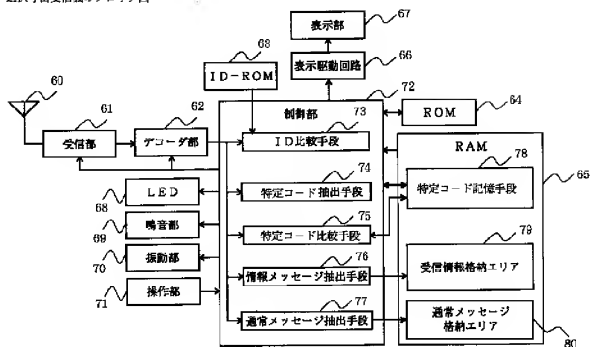
【図 6】

情報メッセージ格納エリア

番号	特定コード	メッセージ内容
1	0 5 0	(天気) に関する情報メッセージ
2	0 0 1	(日本の政治ニュース) に関するメッセージ
3	0 2 2	(スポーツ) に関するメッセージ
4	0 0 3	(日本の政治ニュース)
5	0 0 0	(日本の経済ニュース) に関するメッセージ
6	0 2 2	(スポーツ) に関するメッセージ
.	.	.
.	.	.
N		

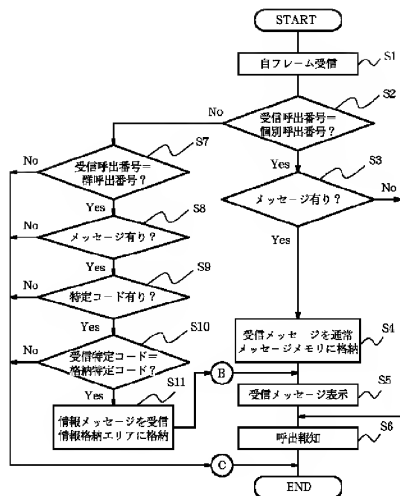
【図 4】

選択呼出受信機のプロック図



【図 7】

選択呼出受信機のフローチャート



JP11331070A

BROADCASTING INFORMATION DISTRIBUTION SYSTEM

Publication number : JP11331070A

Date of publication of application : 30.11.1999

Application number : 11-060433

Applicant : HITACHI LTD

Date of filing : 08.03.1999

Inventor : TANAKA SATOSHI
AMADA EIICHI
MIZUTANI SEKI

Abstract:

PROBLEM TO BE SOLVED: To inexpensively provide information required for each user through a simple procedure by exchanging system control information among plural radio terminals through a control channel and using a radio base station for exchanging user information through a traffic channel allocated to each radio terminal.

SOLUTION: Broadcasting information is distributed while utilizing an exciting radio communication system such as a cellular system. In a content supply system 10, the input and editing operation of content information to be broadcasted is performed. The edited content information is temporarily stored in a storage device 14, transmitted later from communication equipment 15 to a communication line 1 and supplied to respective provider systems 20. At each communication provider system (radio base station BS) 20, the content information is stored in a storage device 24. The content information stored in the storage device 24 is broadcasted from an antenna 31 of radio communication equipment 30 as broadcasting information according to a prescribed broadcasting schedule controlled by a timer 25.

特開平11-331070

(43)公開日 平成11年(1999)11月30日

(51)Int.Cl. ⁶	識別記号	F I		
H 0 4 B 7/26	1 0 1	H 0 4 B 7/26	1 0 1	
G 0 6 F 13/00	3 5 4	G 0 6 F 13/00	3 5 4 D	
H 0 4 Q 7/36		H 0 4 H 1/00	E	
7/38			F	
H 0 4 H 1/00			Z	
審査請求 未請求 請求項の数14 O L (全 17 頁) 最終頁に続く				

審査請求 未請求 請求項の数14 ○ L (全 17 頁) 最終頁に続く

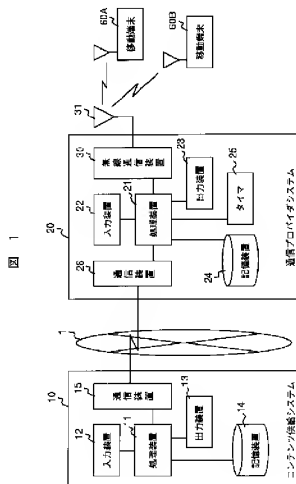
(21)出願番号	特願平11-60433	(71)出願人	000005108 株式会社日立製作所 東京都千代田区神田駿河台四丁目6番地
(22)出願日	平成11年(1999)3月8日	(72)発明者	田中 聡 東京都国分寺市東恋ヶ窪一丁目280番地 株式会社日立製作所中央研究所内
(31)優先権主張番号	特願平10-69729	(72)発明者	天田 栄一 東京都国分寺市東恋ヶ窪一丁目280番地 株式会社日立製作所中央研究所内
(32)優先日	平10(1998)3月19日	(72)発明者	水谷 世希 神奈川県横浜市中区加賀原二丁目2番 株式会社日立製作所ビジネスシステム開発 センタ内
(33)優先権主張国	日本 (J P)	(74)代理人	弁理士 高橋 明夫 (外1名)

(54)【発明の名称】 放送情報配信システム

(57)【要約】

【課題】 複数の無線端末に所望の情報を効率的に配信する情報配信システムを提供する。

【解決手段】 無線基地局が、制御チャネルに同報フレームに関する送信条件を示す同報制御情報を送信し、上記送信条件に従って同報チャネルに同報フレームを送信する。上記同報フレームは、異なるコンテンツ情報を含む複数のサブフレームと、上記各サブフレームのコンテンツ情報に関する案内情報を含んだフレームヘッダとからなり、各無線端末は、制御チャネルで受信した同報制御情報に基づいて、同報チャネルから同報フレームを受信し、上記案内情報に従って、同報フレーム中の特定のサブフレームのコンテンツ情報を選択的に受信する。



【特許請求の範囲】

【請求項1】無線端末との間で、少なくとも1つの制御チャンネルを介して制御情報を交信し、各無線端末に割り当てられたトラヒックチャンネルを介してユーザ情報を交信する少なくとも1つの無線基地局からなる放送情報配信システムであって、

上記基地局が、

上記制御チャンネルに、システム情報と、同報フレームに関する送信条件を定義した同報制御情報とを送信するための制御チャンネル送信回路と、

それぞれトラヒックチャンネルにユーザ情報を送信するための複数のトラヒックチャンネル送信回路と、

上記同報制御情報で定義された特定のチャンネルに、上記送信条件に従って、不特定の無線端末で受信可能な放送情報を含んだ同報フレームを送信するための同報チャンネル送信回路とを備えることを特徴とする放送情報配信システム。

【請求項2】前記同報制御情報が、前記送信条件として、該同報フレームの送信時刻を示す情報を含むことを特徴とする請求項1に記載の放送情報配信システム。

【請求項3】前記同報制御情報が、前記送信条件として、前記同報フレームの送信チャンネルを指定する情報と、前記同報フレームの送信時刻を示す情報とを含むことを特徴とする請求項1に記載の放送情報配信システム。

【請求項4】前記同報フレームが、フレームヘッダと、該フレームヘッダに続く複数のサブフレームとからなり、上記複数のサブフレームが、それぞれ異なる放送情報を含み、上記フレームヘッダは、上記各サブフレームに含まれる放送情報に関する案内情報を含むことを特徴とする請求項1～請求項3の何れかに記載の放送情報配信システム。

【請求項5】前記フレームヘッダが、前記案内情報として、前記各サブフレームに含まれる放送情報の種類を表す分類情報と、上記各サブフレームの送信タイミングを示す時刻情報とを含むことを特徴とする請求項4に記載の放送情報配信システム。

【請求項6】前記各サブフレームは、サブフレームヘッダと、それぞれ放送情報ブロックを含む複数の情報パケットを含むことを特徴とする請求項4に記載の放送情報配信システム。

【請求項7】それぞれ異なる放送情報を含む複数のサブフレームと、上記各サブフレームに含まれる放送情報に関する案内情報を含むフレームヘッダとからなる同報フレームを生成するためのプロバイダと、

無線端末との間で、上り、下りの各方向で少なくとも1つの制御チャンネルを介して制御情報を交信し、上記無線端末に割り当てられた上り、下りの1対のトラヒックチャンネルを介してユーザ情報を交信する無線基地局とからなる放送情報配信システムにおいて、上記無線基地局

が、

下り制御チャンネルに、システム情報と、同報フレームに関する送信条件を定義した同報制御情報とを送信するための制御チャンネル送信回路と、

上記放送情報プロバイダで生成された同報フレームを、上記同報制御情報で定義された特定のチャンネルに、上記送信条件に従って送信するための同報チャンネル送信回路とを有することを特徴とする放送情報配信システム。

【請求項8】前記同報制御情報が、前記送信条件として、前記同報フレームの送信チャンネルを指定する情報と、前記同報フレームの送信時刻を示す情報とを含み、前記同報フレームのフレームヘッダが、前記案内情報として、前記各サブフレームに含まれる放送情報の種類を表す分類情報と、上記各サブフレームの送信タイミングを示す時刻情報とを含むことを特徴とする請求項7に記載の放送情報配信システム。

【請求項9】無線基地局と、複数の無線端末とからなり、上記無線基地局と各無線端末の間で、少なくとも1つの制御チャンネルを介して制御情報を交信し、各無線端末毎に割り当てられた上り方向と下り方向の1対のトラヒックチャンネルを介してユーザ情報を交信する無線通信システムにおいて、
上記無線基地局が、上記制御チャンネルに同報フレームに関する送信条件を示す同報制御情報を送信するための制御チャンネル送信回路と、上記同報制御情報が示す送信条件によって特定される同報チャンネルに、上記送信条件に従って、放送情報供給システムから供給された不特定の無線端末に配信すべき複数の種類の放送情報を含む同報フレームを送信するための同報チャンネル送信回路とを有し、

上記同報フレームが、フレームヘッダと、該フレームヘッダに続く複数のサブフレームとからなり、上記複数のサブフレームが、それぞれ異なる放送情報を含み、上記フレームヘッダが、上記各サブフレームに含まれる放送情報に関する案内情報を含み、

上記各無線端末が、上記制御チャンネルで制御情報を受信する制御チャンネル受信回路と、上記制御チャンネル受信回路で受信された同報制御情報に基づいて、上記同報チャンネルから上記同報フレームを受信し、該同報フレームの案内情報に従って、上記同報フレーム中の特定のサブフレームに含まれる放送情報を選択的に受信するための同報チャンネル受信回路と、上記同報チャンネル受信回路で受信された放送情報を蓄積するための記憶装置と、上記記憶装置に蓄積された放送情報を出力するための出力装置とを有することを特徴とする無線通信システム。

【請求項10】前記同報フレームのフレームヘッダが、前記案内情報として、前記各サブフレームに含まれる放送情報を識別するための情報と、上記各サブフレームの送信タイミングを示す時刻情報とを含み、
前記各無線端末が、上記放送情報のうちの1つを指定す

るための入力装置と、

上記同報フレームのフレームヘッダを受信した後、上記指定された放送情報を含むサブフレームが送信される迄の期間、前記同報チャネル受信回路への電源供給を休止するための電源制御装置とを有することを特徴とする請求項9に記載の無線通信システム。

【請求項11】前記各無線端末の電源制御装置が、前記制御チャネル受信回路で受信された同報制御情報が示す次の同報フレームの送信時刻に従って、前記同報チャネル受信回路を自動的に起動する機能を有することを特徴とする請求項10に記載の無線通信システム。

【請求項12】前記各無線端末が、前記同報チャネル受信回路で受信された放送情報が暗号化されていた場合、前記放送情報供給システムと自動的に交信して、上記暗号化された放送情報を解読するための解読キーを取得するための手段を備えることを特徴とする請求項9〜請求項11の何れかに記載の無線通信システム。

【請求項13】無線基地局との間で、少なくとも1つの制御チャネルを介して制御情報を交信し、各無線端末毎に割り当てられた上り方向と下り方向の一对のトラフィックチャネルを介してユーザ情報を交信する無線端末装置であって、上記制御チャネルで制御情報を受信する制御チャネル受信回路と、

上記制御チャネル受信回路で受信された同報制御情報によって特定される同報チャネルから同報フレームを受信し、該同報フレームに含まれる案内情報に従って、上記同報フレーム中の特定のサブフレームに含まれる放送情報を選択的に受信するための同報チャネル受信回路と、上記同報チャネル受信回路で受信された放送情報を蓄積する記憶装置と、

上記記憶装置に蓄積された放送情報を出力するための出力装置とを有することを特徴とする無線端末装置。

【請求項14】前記同報フレームのフレームヘッダが、前記案内情報として、前記各サブフレームに含まれる放送情報を識別するための情報と、上記各サブフレームの送信タイミングを示す時刻情報とを含み、無線端末が、更に、上記放送情報のうちの1つを指定するための入力装置と、上記同報フレームのフレームヘッダを受信した後、上記指定された放送情報を含むサブフレームが送信される迄の期間、前記同報チャネル受信回路への電源供給を休止するための電源制御装置とを有することを特徴とする請求項13に記載の無線端末装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は情報配信システムに関し、更に詳しくは、無線通信システムの基地局から放送情報を送信し、各無線端末においてユーザによって予約された情報を自動的に収集できるようにした放送情報配信システム、無線通信システム、および無線端末装置

に関する。

【0002】

【従来の技術】通信回線を利用したコンピュータネットワークでは、各端末ユーザが宛先装置との間に個別の双方向回線を設定することによって、所望の情報サイトから必要な情報を引き出すことが可能である。例えば、端末装置とインターネット接続装置との間に双方向回線を設定すれば、任意のWEBから情報を引き出し、端末装置に表示することが可能である。

【0003】

【発明が解決しようとする課題】しかしながら、従来の通信ネットワークで所望の情報提供装置をアクセスするためには、各端末ユーザが、端末装置と上記情報提供装置との間に通信回線を設定するための複雑な通信手順を実行する必要があり、所望の情報を取得する迄に時間がかかると言う問題がある。また、情報提供システムから端末への情報の送信は、各ユーザ端末毎に確立された専用の通信チャネルを介して行われるため、所望の情報入手に必要な通信料金が高額になるという問題がある。上述した問題は、携帯電話やPHS (Personal Handyphone System) などの無線通信システムの端末装置が、無線チャネルを介して情報提供装置をアクセスする場合に特に顕著になる。

【0004】尚、不特定多数の車載ラジオに対して、道路の混雑状況を示す交通情報などの報知情報を放送する情報報知システムとして、例えば、特開平10-22951号公報では、送信機から、それぞれがIDヘッダと、複数の情報エレメントに分割された情報データと、EODとからなる複数グループの報知情報を周波数変換して繰り返して放送し、受信機側で、受信した全ての情報グループをメモリに記憶し、視聴者が操作パネルで選択した区分の情報グループをメモリから読み出し、周波数逆変換してスピーカに出力することによって、視聴者が放送時間帯に関係なく報知情報を聞けるようにしたシステム構成が公知となっている。上記公報に記載のシステムでは、放送された全ての情報グループを受信機側で記憶することを前提としており、特定グループの情報を選択的に受信することができない。

【0005】本発明の目的は、各ユーザが必要とする情報を簡単な手順で、安価に提供できる情報配信システムおよび無線通信システムを提供することにある。本発明の他の目的は、電池で動作する移動端末のユーザに対して、電池の消耗をできるだけ抑制して、所望の情報を効率的に配信できる情報配信システムおよび無線通信システムを提供することにある。本発明の他の目的は、端末ユーザが、所望の情報を自分に都合の良いタイミングで参照可能な放送情報配信システムおよび無線通信システムを提供することにある。本発明の更に他の目的は、有料情報に対する課金に適した放送情報配信システムおよび無線通信システムを提供することにある。本発明の更

に他の目的は、情報を複数のユーザ端末に効率良く配信できる無線基地局、および、ユーザが所望する情報を効率良く受信できる無線端末装置を提供することにある。

【0006】

【課題を解決するための手段】上記目的を達成するために、本発明の情報配信システムは、複数の無線端末との間で、少なくとも1つの制御チャネルを介してシステム制御情報を交信し、各無線端末に割り当てられたトラヒックチャネルを介してユーザ情報を交信する無線基地局を利用する。本発明で利用する無線基地局は、上記制御チャネルに、システム制御情報と同報フレームに関する送信条件を定義した同報制御情報とを送信するための制御チャネル送信回路と、上記同報制御情報で定義された特定のチャネルに、上記送信条件に従って、不特定の無線端末で受信可能な放送情報を含んだ同報フレームを送信するための同報チャネル送信回路とを備えたことを特徴とする。

【0007】例えば、CDMA(Code Division Multiple Access)技術を用いたセルラシステムの場合、無線チャネルは、送信情報のスペクトル拡散に使用される拡散コードによって特定できる。送信側で或る拡散コードによってスペクトル拡散された送信信号は、受信側で同一の拡散コードを使用して逆拡散した場合にのみ、受信可能である。従って、無線基地局から各端末に、同報チャネルで使用する拡散コードや伝送速度等のチャネル情報を予め通知することができれば、全ての端末が同報チャネルの送信情報を受信することができる。

【0008】本発明によれば、制御チャネルに送信する同報制御情報によって、各端末に同報チャネルのチャネル情報を通知することにより、基地局セル内に位置する全端末が放送情報を受信可能となる。また、本発明によれば、セルラシステム等の無線通信システムのインフラを利用して、各無線基地局から放送情報を送信するようにしているため、各無線基地局のカバーエリアに応じて、地域的に特徴のある放送情報を無線端末に配信することができる。無線基地局から、同一内容をもつ同報フレームを周期的に複数回放送し、各、無線端末が、伝送エラーにより正常受信できなかった放送情報を次の同報フレームで再度受信することによって、信頼性の高い情報配信が可能となる。

【0009】本発明の他の特徴は、上記同報制御情報で、同報チャネル（または拡散コード）の指定情報の他に、同報フレームの送信時刻を示す情報を含み、各同報フレームが、それぞれ異なる放送情報を含む複数のサブフレームと、上記各サブフレームのコンテンツ（放送情報）に関する案内情報を含むフレームヘッダとから構成されたことにある。上記各サブフレームは、例えば、サブフレームヘッダと、放送情報ブロックを含む複数の情報パケットからなる。

【0010】本発明の放送情報配信システムを利用する

各無線端末は、制御チャネルで制御情報を受信する制御チャネル受信回路と、上記制御チャネル受信回路で受信された同報制御情報に基いて、上記同報チャネルから上記同報フレームを受信し、同報フレームヘッダが示す案内情報に従って、上記同報フレーム中の特定のサブフレームに含まれる放送情報を選択的に受信するための同報チャネル受信回路と、上記同報チャネル受信回路で受信された放送情報を蓄積するための記憶装置と、上記記憶装置に蓄積された放送情報を出力するための出力装置とを有することを特徴とする。

【0011】本発明の他の特徴は、上記同報フレームヘッダが、案内情報として、各サブフレームに含まれる放送情報の特徴、例えばコンテンツ名称と、上記サブフレームの送信タイミングを示す時刻情報とを含み、各無線端末が、受信すべき放送情報を指定するための入力装置と、上記同報フレームのフレームヘッダを受信した後、上記指定された放送情報を含むサブフレームが送信される迄の間、同報チャネル受信回路への電源供給を休止するための電源制御装置と備えた構成にある。上述したように、制御チャネルで同報フレームの送信時刻を予告することによって、各端末は、次の同報フレームの先頭が到来する迄、同報チャネルの受信回路を休止させることができる。また、各端末が、予めユーザが予約した放送情報の識別子を記憶しておき、フレームヘッダの受信を完了した時点で同報チャネル受信回路を一旦休止状態にし、上記予約された放送情報を含む目的サブフレームの送信タイミングで同報チャネル受信回路を起動することによって、電池の消耗を防ぐことができる。

【0012】本発明による無線端末は、同報チャネル受信回路で受信された放送情報が暗号化されていた場合、放送情報供給システムと自動的に交信して、暗号化放送情報の解読に使用する解読キーを取得するための手段を備えたことを更に他の特徴とする。上記同報チャネルのように、複数の端末に共通のチャネルを利用した情報配信システムでは、配信情報に対する課金方法が問題となるが、有料情報を暗号化し、且つ、同報チャネルとは別の双方向チャネルを使用して各端末毎に解読キーを配布するようにすれば、放送情報供給システム側で、有料放送情報の利用者に対する個別的な課金が可能となる。

【0013】

【発明の実施の形態】図1は、本発明による放送情報配信システムの全体的な構成を示す。図1において、10は、放送情報となる各種のコンテンツを生成するためのコンテンツ供給システム、20は、公衆ネットワークまたは専用線などからなる通信網1を介して上記コンテンツ供給システム10に接続された通信プロバイダ・システムを示す。上記通信プロバイダ・システム20は、コンテンツ供給システム10から受信した放送情報を、無線通信装置30を介して、複数のユーザ端末、例えば、移動端末MS6.0(6.0A〜6.0N)に放送する。

【0014】本発明は、セルラシステムなどの既存の無線通信システムを利用して放送情報を配信するものであり、上記通信プロバイダ・システム20は、セル無線通信システムを構成する無線基地局BSに組み込まれる。図1では、1つの放送情報プロバイダ・システム20しか示していないが、実際の応用では、上記コンテンツ供給システム10で編集された放送情報が、通信網1と、該通信網の一部を構成する移動交換機および無線基地局制御装置を介して、複数の無線基地局BSに配布される。上記放送情報は、各無線基地局BSに付随した通信プロバイダ・システム20の記憶装置に蓄積され、無線基地局BSの無線通信装置を介して無線端末に放送される。

【0015】コンテンツ供給システム10では、処理装置11に接続された入力装置12と、ディスプレイなどの出力装置13を使用して、放送すべきコンテンツ情報の入力と編集操作が行われる。編集されたコンテンツ情報は、記憶装置14に一時的に記憶された後、通信装置15から通信回線1に送信され、各プロバイダシステム20に供給される。各通信プロバイダ・システム（無線基地局BS）20では、上記コンテンツ供給システム10から送信されたコンテンツ情報を通信装置26によって受信し、記憶装置24に蓄積する。上記記憶装置24に記憶されたコンテンツ情報は、タイマー25で制御される所定の放送スケジュールに従って、無線通信装置30のアンテナ31から放送情報として放送される。尚、記憶装置24に記憶されたコンテンツ情報は、必要に応じて、入力装置22からのオペレータ操作によって出力装置23に出力され、チェックまたは編集が加えられる。

【0016】本発明では、セルラ無線基地局BSから移動端末60に向かう下り方向のトラフィックチャネルのうちの1つを同報チャネルとして使用し、この同報チャネルで放送情報を送信することにより、単一の物理チャネルで不特定多数の無線端末に同時に放送情報を配布することを特徴としている。同報型情報サービスは、第3世代移動通信システムでも検討されているが、具体的な構造提案に至っていない。本発明は、物理的に全端末が全チャネルを受信できるという無線通信システムの特性を活かし、現状のパケット通信を更に拡張することにより、多数のユーザに比較的情報量の多い同報コンテンツ情報を効率的に配布することを可能とする。

【0017】エンドユーザが使用する無線端末60としては、セルラシステムなどの無線通信システムの一部を構成している既存の移動端末に、同報チャネルで送信される放送情報を受信するための機能と、エンドユーザが所望するコンテンツの識別子を予約するための機能と、放送情報の中から予約されたコンテンツを選択的に受信して記憶装置に蓄積するための機能と、エンドユーザからの要求に応じて、蓄積されたコンテンツを出力するた

めの機能とを付加したものが使用される。本発明では、後述するように、1つの同報フレームで、それぞれが比較的多くの情報量を持つ複数種類のコンテンツ情報を放送する。上記同報フレームは、各基地局BSからを繰り返して送信されるが、放送情報量が多いため、同報フレームの繰り返し周期は比較長くなる。

【0018】図2は、本発明において、各基地局BSから送信される制御フレームのフォーマットを示す。制御フレーム100は、通常の無線通信システムで基地局から移動端末に送信すべきシステム情報101の他に、本発明に特有の制御情報として、同報チャネルを特定するための同報チャネルパラメータ102と、次の同報フレームの送信時刻（以下、同報時刻と言う）103とを示す同報制御情報を含んでいる。

【0019】図3は、上記同報チャネル識別子102で指定された下りチャネル（以下、同報チャネルと言う）で、上記送信時刻103に送信が開始される同報フレーム200のフォーマットを示す。同報フレーム200は、フレームヘッダ210と、複数のサブフレーム220（220A～220K）とからなる。本発明では、上記サブフレーム毎に異なった種類のコンテンツ情報を送信する。図示した例では、1つの同報フレーム200でK種類のコンテンツ情報が、同報情報としてサービスされる。サブフレーム220A～220Kに含まれるコンテンツの種類は、フレームヘッダ210で示される。

【0020】各サブフレーム220の先頭には、サブフレームの開始と該サブフレームに含まれるコンテンツ情報の識別子を示すサブフレームヘッダ221が位置し、上記サブフレームヘッダ221の後は、複数個のパケット222（222A～222L）が続き、サブフレームの最後には、サブフレーム220の終了を示す終了フラグ224が位置している。各パケット222には、パケット単位で受信誤りを検出できるように、CRC（Cyclic Redundancy Check）223（223A～223L）が付加されている。

【0021】同報フレームヘッダ210は、図4に示すように、フレーム定義フィールド211と、サブフレーム220A～220Kと対応した複数のビットからなる更新コンテンツ表示フィールド212と、サブフレーム220A～220Kと対応した複数個の固定長のコンテンツ案内フィールド213（213A～213K）とからなる。

【0022】上記フレーム定義フィールド211は、フレームヘッダ210の長さ、該フレームヘッダのフォーマットを示す定義情報を含む。また、上記各コンテンツ案内フィールド213は、これと対応するサブフレーム220に含まれるコンテンツ情報を識別するためのコンテンツ識別子301と、コンテンツ名302と、コンテンツ情報の放送開始時刻303と、そのコンテンツ情報が有料か無料かを示す表示304と、有料コンテン

の場合の課金条件305と、コンテンツ情報のバージョン識別子306と、コンテンツのデータ長307とを含む。

【0023】上記課金条件305は、例えば、暗号化された有料コンテンツ情報を復号化するために必要な解読キーの有効期限と料金を示す。現在保持している解読キーが有効期限切れとなった端末装置は、コンテンツ供給システム10に対して新たな解読キーの送信を要求する。コンテンツ供給システム10は、端末装置からコンテンツIDを指定して新たな解読キーの送信要求を受けた時、上記端末装置に対して、要求日から上記解読キーの有効期限日までのサービス料金を課金する。

【0024】上記放送開始時刻303は、コンテンツ案内213と対応したサブフレーム220の放送開始時刻を示しており、この時刻をセルラシステムに固有のシステムクロックによって指定するようにすれば、同報フレームを送信する基地局BS側とこれを受信する移動端末側の同期が容易となる。また、上記バージョン識別子306としては、例えば、更新されたコンテンツ情報の最初の放送日時を適用する。コンテンツ情報が更新されたか否かは、更新表示ビットパターン212からも判定できるが、各端末が、同報フレームヘッダ210の受信の都度、既に入手済みのコンテンツのバージョン識別子と、上記同報フレームヘッダ210が示すバージョン識別子306とを比較すれば、上記同報フレームのコンテンツ情報が受信済みのものか否かを判断できる。

【0025】図5は、基地局BSと移動端末60との間に形成される無線チャンネルの構成を示す。CDMA(Code Division Multiple Access)方式のセルラシステムでは、基地局BSと各移動端末60との間に、基地局から端末へ向かう下りチャンネルとして、3つの制御チャンネルと、ユーザ情報送信用の1つのトラヒックチャンネルが使用され、端末から基地局へ向かう上りチャンネルとして、2つの制御チャンネルと、ユーザ情報送信用の1つのトラヒックチャンネルが使用される。

【0026】図5において、下り共通制御チャンネルCCH1は、例えば、セル情報、同期情報、他の制御チャンネルで使用するべき拡散コードなど、無線システムの制御に必要なシステム情報を全ての端末に共通に送信するために使用される。上記下り共通制御チャンネルCCH1自体の拡散コードは、各移動端末側で、予め定められたアルゴリズムによって特定できる。上り共通制御チャンネルCCH1は、端末からの発信を基地局に通知するためのものであり、全ての端末で共通に使用される。下り共通制御チャンネルCCH2は、端末への着信通知と、端末への下り個別制御チャンネルCCH3の割り当て制御に使用され、下り個別制御チャンネルCCH3と上り個別制御チャンネルCCH2は、着信通知後の端末と基地局との間で、接続制御情報の送受信に使用される。これらの制御チャンネルの他に、基地局BSは、異なる2n種類の拡散コ

ードを使用することによって、下り方向と上り方向にそれぞれn個のトラヒックチャンネルTCH1～TCHnを形成し、着信端末または発信端末に対して、下り方向と上り方向の1対のトラヒックチャンネルTCHiを割り当てる。

【0027】本発明では、上述した従来のセルラシステムにおけるチャンネル構成に、下り方向の同報チャンネルBCHを追加し、この同報チャンネルを利用して、通信プロバイダシステム20が出力した同報フレーム200を放送する。トラヒックチャンネルTCH用の拡散符号のうちの1つを同報チャンネルに割り当てても良い。上記同報チャンネルBCHで使用する拡散コードや、同報フレーム200の放送開始時刻などの同報制御情報は、図2の制御フレーム100に示したように、下り共通制御チャンネルCCH1で送信される制御フレーム100の一部として送信することによって、各端末に同報チャンネルBCHの受信を可能とする。

【0028】CDMAセルラシステムにおいて、上記同報チャンネルBCHは、電力制御を必要としないと言う点を除いて、他のトラヒックチャンネルTCHと同様の物理的構成で済む。また、端末側では、上記同報チャンネルBCHは、通常のトラヒックチャンネルと同様の受信回路で受信可能である。各端末でユーザがトラヒックチャンネルTCHで通話中に、同報チャンネルBCHから同報フレーム200を受信できるようにするためには、各端末に、トラヒックチャンネルTCH用の受信回路とは別に共通チャンネルBCH専用の受信回路を設ける必要がある。ユーザが通話中は同報フレームの受信を中断することになれば、通常のトラヒックチャンネル用の受信回路で拡散コードを切り替えることによって、上記同報フレームを受信できる。

【0029】図6は、上述した同報チャンネルBCHを介して同報フレーム200を送信する機能を備えた本発明による無線基地局BSの1実施例を示す。基地局BSは、基地局制御装置50と通信するための通信装置(回線インタフェース)26と無線通信装置30とに接続された内部バス40を有し、この内部バス40に接続して、基地局の動作を制御するための処理装置33と、上記処理装置33が実行する各種の制御プログラムとデータを格納するためのメモリ34を備えている。

【0030】図1で示した通信プロバイダ20の機能は、上記基地局を構成する処理装置33で実現できるが、図6の実施例では、ブロックSPで示すように、基地局BSに必要な一般的な機能を果たす処理装置33とは別に、上記通信プロバイダ20の機能を担う処理装置21を設けた構成としている。コンテンツ供給システム10で生成されたコンテンツ情報は、通信網から移動交換局51を介して基地局制御装置50に送信され、上記基地局制御装置50によって複数の基地局BSに配布される。各基地局BSでは、上記コンテンツ情報を通信装

置26と内部バス40とインタフェース47を介して、上記通信プロバイダSPの記憶装置24に転送する。

【0031】各基地局BSの無線通信装置30は、複数の送信回路35A～35Cおよび36と、複数の受信回路37A、37Bを含む。送信回路35Aは下り共通制御チャネルCCH1用、送信回路35Bは下り共通制御チャネルCCH2用のものであり、これらの送信回路は、内部バス40を介して接続された処理装置33から、送信すべき制御情報を受信する。尚、信号線41Aと41Bは、上記各送信回路35A、35Bで使用するべき拡散符号を指定するための制御信号線を示す。

【0032】送信回路35Cは、下り個別制御チャネルCCH3用とトラヒックチャネルTCH用に兼用され、複数のトラヒックチャネルに対応して複数の送信回路が用意されている。これらの送信回路35Cは、処理装置33から内部バス40を介して制御信号線41Cに出力される拡散符号の指定信号によって、下り個別制御チャネルCCH3からトラヒックチャネルTCHへ、あるいはその逆のチャネル切替が行われる。また、これらの送信回路41Cは、回線インタフェース32に接続されており、下り個別制御チャネルCCH3として使用中は、基地局制御装置50あるいは該制御装置50に接続された移動交換局が発生する接続制御信号を送信し、トラヒックチャネルTCHとして使用中は、通信相手装置から基地局制御局50を経由して受信された通話信号を送信する。

【0033】送信回路36は、本発明に特有の同報チャネルBCH用のものであり、インタフェース回路46を介して通信プロバイダSPから同報フレームを受信し、これを制御信号線42で指定された拡散符号で符号拡散（スペクトル拡散）して送信する。上記各送信回路35A～35Cおよび36からの出力されたスペクトル拡散信号は、合成回路38によって合成された後、無線部39で発生する所定周波数のキャリア信号に重畳され、アンテナ31から無線信号として送信される。

【0034】一方、アンテナ31からの受信信号は、キャリア選択、周波数変換、フィルタリング、アナログ/デジタル変換機能を持つ無線部39を通過した後、受信回路37Aと複数の受信回路37Bに入力される。受信回路37Aは、上り共通制御チャネルCCH1の制御信号を受信し、受信した制御信号を内部バス40を介して処理装置33に転送する。また、各受信回路37Bは、上り個別制御チャネルCCH2の制御信号とトラヒックチャネルTCHの信号を受信し、これらの受信信号を通信装置32を介して基地局制御装置50に転送する。これらの受信回路37A、37Bの受信チャネルは、処理装置33から信号線43A、43Bに与えられる拡散符号指定信号によって決まり、受信回路38Bにおける受信チャネルCCH1からTCHへの切り替えは、逆拡散に使用する拡散符号を切り替えることによ

て達成される。

【0035】通信プロバイダSPは、内部バス40に接続されたインタフェース回路47を介して基地局処理装置33と通信し、処理装置33が下り共通制御チャネルCCH1で移動端末に通知する同報時刻103に同期して、次の同報フレーム200をインタフェース回路46を介して同報チャネル送信回路に送出する。なお、同報フレームを可変長とし、先行フレームと後続フレームとの送信間隔を調整することにより、同報フレームの送信を所定の周期で繰り返すようにすれば、処理装置33とプロバイダSPとの間の同期制御が容易になる。

【0036】図7は、移動端末60の構成の1例を示す。移動端末60は、内部バス70に接続された処理装置63と、上記処理装置が実行する各種のプログラムおよびデータを記憶するためのメモリ64と、送信回路65と、複数の受信回路66A～66Cと、電源制御回路67を備える。

【0037】送信回路65は、上り方向の共通制御チャネルCCH1と、個別制御チャネルCCH2と、トラヒックチャネルTCHに共用され、これらのチャネル間の切り替えは、処理装置63から信号線71に与えられる拡散符号指定信号に応じて行われる。制御チャネルCCH1用またはCCH2用として動作中は、処理装置63から内部バス70に出力された制御情報がセクタ73を介して送信回路65に供給され、トラヒックチャネルTCH用として動作中は、音声符号化復号化回路81で符号化されたマイクロホン82からの入力音声が入記セクタ73を介して送信回路65に供給され、送信回路でスペクトル拡散された送信信号は、無線部69で所定のキャリア周波数に重畳された後、アンテナ61から無線信号として送出される。

【0038】受信回路66Aは、下り共通制御チャネルCCH1に専用の受信回路、受信回路66Bは、共通制御チャネルCCH2と、個別制御チャネルCCH3と、トラヒックチャネルTCHとに共用の受信回路、受信回路66Cは、同報チャネルBCHに専用の受信回路であり、これらの受信回路は、処理装置63から信号線72A、72B、72Cに与えられる逆拡散符号指定信号に応じて受信チャネルを選択する。受信回路66Aからの受信信号は、内部バス70を介して処理装置63に取り込まれ、受信回路66Bからの出力信号は、受信回路が制御チャネル用として動作中は内部バス40を介して処理装置63に取り込まれ、トラヒックチャネル用として動作中は、セクタ74を介して音声符号化復号化回路81に供給され、復号化された音声信号がスピーカ83に出力される。受信回路66Cで選択的に受信された放送情報は、内部バスを介して記憶装置80に蓄積される。

【0039】移動端末60は、ユーザインタフェースとして、着信を通知するためのベル84と、文字情報を表

示すための表示装置 85 と、テンキーその他のファンクションキーを含む入力装置 86 と、外部の記憶装置やコンピュータ装置と接続するためのインタフェース回路 87 を備えている。放送情報記憶用の記憶装置 80 は、例えば、フラッシュメモリ等の比較的大容量のメモリであり、記憶装置 80 から読み出された放送情報は、内部バス 70 を介して、音声符号化復号化回路 63 または表示装置 85 に出力される。

【0040】電源制御回路 67 は、移動端末の構成要素となる上述した各種の回路部分への電源電圧の供給を選択的に制御するためのものであり、移動端末が待ち受け状態にある間は、電池の消耗をできるだけ抑えるために、処理装置 63 や共通制御チャネル CCH1 の送受信回路等の必要要素を残して、他の回路への電源供給を停止する。後述するように、同報チャネルの受信回路 66 C は、フレームヘッダ 210 とユーザが予約した放送コンテンツ情報を含む特定のサブフレームの受信期間を除いて、電源の供給が停止される。

【0041】図 8 は、基地局の無線通信装置 30 に含まれる送信回路 35 の基本的構成を示す。移動端末 60 を構成する送信回路 65 も基本的に同様の構成からなる。インタフェース回路 351 に入力された送信情報は、送信データバッファメモリ 352 を介して、誤り訂正符号器 353 に供給される。上記誤り訂正符号器 353 は、インターリーブ (interleaver) と、ターボ符号器または畳み込み符号器からなる。上記誤り訂正符号器 353 で訂正符号化された送信信号は、変調回路 354 に入力され、所定の変調処理を受けた送信信号が符号拡散回路 355 に入力される。符号拡散回路 355 は、入力信号を拡散符号発生器 356 から出力された拡散符号によって符号拡散 (スペクトル拡散) した後、無線回路 39 に出力する。上記拡散符号発生器 356 は、処理装置が信号線 41 に出力した拡散符号指定信号に応じた拡散符号を上記符号拡散回路 355 に供給する。

【0042】図 9 は、基地局の無線通信装置 30 に含まれる受信回路 37 の基本的構成を示す。移動端末の受信回路 66 も基本的にはこれと同様の構成からなる。無線回路 39 から入力された受信信号は、逆拡散回路 371 に入力され、逆拡散符号発生器 372 から与えられた拡散符号で逆拡散した後、検波回路 373 に入力される。上記拡散符号は、信号線 43 から与えられた符号指定信号によって決まる。検波回路 373 で所定の復調処理を受けた受信信号は、誤り訂正復号器 374 で誤り訂正した後、受信データバッファメモリ 375 に一時的に蓄積され、インフェース回路 376 を介して内部バス 40 に出力される。上記誤り訂正復号器 374 は、デインターリーブ (deinterleaver) と、ターボ復号器またはビット復号器とからなる。

【0043】図 10 は、同報フレームヘッダ 210 の受信時に移動端末 60 が形成するコンテンツ案内テーブル

(TBL1) 400 の構成を示す。コンテンツ案内テーブル 400 は、同報フレームヘッダ 210 に含まれるコンテンツ案内フィールド 213A~213K と対応した複数のレコードからなり、各レコードは、コンテンツ案内フィールド 213 に含まれるデータ項目 301~307 と対応した複数のデータ項目 401~407 からなる。

【0044】図 11 は、移動端末 60 が形成するコンテンツ予約テーブル (番組予約テーブル TBL2) 500 の構成を示す。コンテンツ予約テーブル 500 は、ユーザが移動端末で予約操作した時に形成され、予約された放送コンテンツ情報と対応した少なくとも 1 つのレコードからなる。各レコードは、予約番号 501 と、コンテンツ ID 502 と、有料/無料表示 503 と、バージョン識別子 504 と、記憶装置 80 に蓄積されたコンテンツ情報を読み出すためのファイルポインタ (またはファイル名称) 505 と、コンテンツがエラーなく受信できたか否かを示す完了表示 506 と、暗号化コンテンツの解読に必要な暗号解読キー 507 と、解読キーの有効期限 508 とを含む。

【0045】尚、暗号解読キーの実体は別の記憶エリアに格納しておき、フィールド 507 には上記解読キーを読み出すためのポインタを記憶するようにしてもよい。これらの項目のうち、項目 501~503 のデータは、ユーザが予約操作した時にサーバ案内テーブル 400 から複写され、その他の項目のデータは、後述するように、同報チャネル BCH から目的のコンテンツ情報を受信した時点で設定される。

【0046】図 12 は、移動端末 60 の処理装置 63 が実行する同報放送情報受信プログラムのフローチャートを示す。移動端末の主電源がオン状態 110 になった時、受信回路 66 A で共通制御チャネル CCH1 から受信される制御フレーム 1100 から同報制御情報を抽出し (ステップ 111)、同報時刻 103 をタイマ T1 に設定する (ステップ 112)。同報時刻になって、タイマ T1 の割込み 120 が発生すると、同報チャネル BCH の受信回路 66 C を起動し、同報フレームのフレームヘッダ 210 を受信し (ステップ 121)、上記フレームヘッダに含まれるコンテンツ案内 213 に従って、図 10 に示したコンテンツ案内テーブル (TBL1) 400 を形成する (ステップ 122)。

【0047】次に、予約テーブル (TBL2) のレコードを指定するためのパラメータ p の値を初期値 0 に設定し (ステップ 123)、パラメータ p の値をインクリメント (ステップ 124) した後、予約テーブル 500 の第 p 番目のレコード TBL2 (p) に予約データがあるか否かを判定する (ステップ 125)。もし、予約データがあった場合は、予約されたコンテンツが既に入手済みか否かを判定する (ステップ 126)。上記判定は、予約レコード TBL2 (p) に含まれるバージョン識別

子504と、コンテンツ案内テーブル400において上記予約レコードTBL2(p)と同一コンテンツIDをもつレコードTBL1(j)のバージョン識別子406とを比較し、予約レコードTBL2(p)の完了表示506をチェックすることによって達成される。

【0048】予約レコードTBL2(p)と案内レコードTBL1(j)のバージョン識別子が一致し、完了表示506に完了フラグが設定してあった場合は、目的のコンテンツが既に入手済みとなっている。この場合は、ステップ124に戻って、次の予約レコードについて同様の判定を繰り返す。バージョン識別子が不一致の場合、または、完了表示506に完了フラグが未設定の場合は、上記案内レコードTBL1(j)の放送開始時刻403をタイムT2に設定し(ステップ127)、上記案内レコードTBL1(j)のバージョン識別子406を書き換えて予約レコードTBL2(p)のバージョン識別子504に書き込み、完了表示505をクリア(ステップ128)した後、同報チャネル受信回路66Cへの電源供給をストップし(ステップ129)、タイム割込みを待つ。

【0049】ステップ125で、予約レコードTBL2(p)に予約データがなければ、現在の同報フレームでこれ以上受信動作する必要がないため、同報チャネル受信回路66Cへの電源供給をストップし(ステップ130)、後述する暗号解読キー入手処理ルーチン(ステップ150)を実行した後、前述した同報制御情報の受信ステップ111、112を実行する。

【0050】タイムT2の割込み140が発生すると、同報チャネル受信回路66Cを起動し、予約レコードTBL2(p)と対応する目的コンテンツの情報パケットを含むサブフレーム220の受信を開始する(ステップ141)。受信された情報パケット222は、順次に記憶装置80に蓄積し(ステップ143)、サブフレームの終了フラグ224が検出された時(ステップ142)、予約レコードTBL2(p)にファイルポインタ505を設定し、完了表示506に完了フラグを設定(ステップ145)した後、ステップ124に戻って、次の予約レコードについて上述した動作を繰り返す。なお、受信パケットに訂正不能なエラーが発生した場合は、次の同報フレームで同一コンテンツを再受信する必要があるために、完了表示506にフラグは設定しない。

【0051】以上のプログラム動作によって、各移動端末60は、基地局BSが同報チャネルBCHに新たな同報フレーム200を送信する都度、タイムT1割込みによってコンテンツ案内情報を受信し、タイムT2割込みによって目的のコンテンツ情報を選択的に受信できる。また、同報フレームの全長に対してユーザが所望する目的の放送情報の占める割合が著しく低い場合でも、不要情報の送信期間は同報チャネル受信回路への電源供給を

ストップすることにより、電池の消耗を抑制しつつ、ユーザが所望する最新の放送情報を記憶装置80に蓄積できる。

【0052】図13は、暗号解読キー入手処理ルーチン150の詳細を示す。このルーチン150は、受信完了したコンテンツが暗号化された有料コンテンツの場合に、コンテンツ供給システム10から解読キーを入手するためのものである。予約テーブル500のレコードを特定するためのパラメータpを初期化しておき(ステップ151)、上記パラメータpの値をインクリメント(ステップ152)した後、p番目の予約レコードTBL2(p)に予約データがあるか否かを判定する(ステップ153)。予約データがあった場合は、まず、有料表示503と完了表示506を判定する(ステップ154)。予約されたコンテンツが無料、または正しく受信されていなかった場合は、ステップ152に戻り、次の予約レコードについて、上述した判定を繰り返す。

【0053】有料コンテンツを正しく受信していた場合は、予約レコードTBL2(p)の解読キーの有効期限508をチェックする(ステップ155)。解読キーの有効期限が切れていなければ、ステップ152に戻って、次の予約レコードについて、上述した判定を繰り返す。解読キーの有効期限が切れているか、あるいは、有効期限508にデータが未設定の場合は、コンテンツ供給システム10から新たな解読キーを入手する必要がある。

【0054】この場合、まず、コンテンツ供給システム10と端末との間の回線が接続済みか否かをチェックし(ステップ157)、回線が未接続の場合は、予め記憶されている電話番号を自動発呼し、セルラの一般の通信回線を介してコンテンツ供給システム10と接続する(ステップ158)。コンテンツ供給システム10からの応答によって回線が接続されたことを確認すると、コンテンツID502と端末識別子(電話番号)を含む暗号解読キー要求メッセージを送信する(ステップ159)。また、相手装置から暗号解読キーを含むメッセージを受信すると、これを予約レコードTBL2(p)の解読キー507として記憶し(ステップ160)、解読キーを受信したことを示す応答メッセージを送信(ステップ161)した後、ステップ152に戻る。解読キーを正常に受信できなかった場合は、再度、暗号解読キー要求メッセージを送信する。

【0055】ステップ153で、予約レコードTBL2(p)に予約データがない場合、回線が接続中か否かをチェックし(ステップ162)、回線が接続中であれば、これを切断(ステップ163)した後、このルーチンを終了する。尚、コンテンツ供給システム側では、端末装置60がステップ161で送信した応答メッセージを受信すると、メッセージの受信日から解読キーの有効期限日までのコンテンツ情報の使用料金を計算し、要求元のユーザ(端末装置の電話番号)に課金する。図14

は、ユーザからのコンテンツ予約要求に回答して移動端末60が実行するプログラムのフローチャートを示す。入力装置86からコンテンツ予約要求を受けると、コンテンツ案内テーブル400を参照して、表示装置85に予約画面を表示する(ステップ601)。予約画面には、ユーザが所望のコンテンツを選択するのに必要な情報として、例えば、上記コンテンツ案内テーブル400におけるコンテンツID401、コンテンツ名称402、有料表示403、課金条件405を含むエントリを表示する。また、既に予約テーブル500に予約レコードが登録済みの場合は、予約レコードと対応するエントリに該当コンテンツが予約済みであることを示すマークを表示する。

【0056】小型の移動端末では表示画面のサイズに制約があるため、端末の表示画面には、予約画面を構成する複数のエントリを順次にスクロールして表示することが望ましい。上記予約画面を表示中に、所望コンテンツのエントリをユーザが選択操作した時、これと対応する予約レコードを予約テーブル500に生成する(ステップ603)。ユーザが予約終了を示す入力操作を行った場合は(ステップ602)、このルーチンを終了する。

【0057】図15は、ユーザからの放送情報出力要求に回答して移動端末60が実行するプログラムのフローチャートを示す。入力装置86から放送情報出力要求を受けると、表示装置85にコンテンツ選択画面を表示し(ステップ611)、ユーザがコンテンツを指定するのを待つ(ステップ612)。コンテンツ選択画面としては、例えば、予約テーブルの各予約レコードと対応して案内テーブル400から読み出されたコンテンツ名称402を表示する。

【0058】コンテンツ選択画面の表示中に、ユーザがコンテンツの選択操作を行うと、選択されたコンテンツが有料か否かをチェックし(ステップ613)、もし、有料コンテンツの場合は、このコンテンツと対応する解読キー508を読み出し、暗号解読の準備をしておく(ステップ614)。次に、予約テーブル500に記憶されているファイルポインタ504に基づいて、記憶装置80から目的のコンテンツ情報の読み出しを開始し、順次に出力装置に出力する(ステップ615~616)。目的のコンテンツ情報が暗号化されている場合は、記憶装置80から読み出された情報を次々と解読しながら、出力装置に転送する。上記出力装置へのコンテンツの転送は、記憶装置から目的コンテンツの全ての情報を読み終えるまで繰り返される(ステップ617)。

【0059】図6に示した実施例では、通信プロバイダSPを基地局BSの処理装置33とは別の処理装置21で構成したが、上記通信プロバイダの機能と基地局機能とを同一の処理装置33で実現したい場合は、記憶装置24を内部バス40に結合し、処理装置33によって上記記憶装置24から同報フレームを読み出し、これを内

部バス40を介して同報チャンネル送信回路36に供給するようにすればよい。

【0060】また、実施例では、各無線基地局BSに通信プロバイダ機能SPを装備したが、通信プロバイダ機能を基地局制御装置50に装備してもよい。この場合、基地局制御装置50が同一の同報フレームを複数の基地局BSに配布し、各基地局が、ユーザトラヒックの1つとして基地局制御装置から受信した同報フレームを同報チャンネル送信回路に送出する。また、基地局制御装置から制御情報として別途通知された同報フレーム放送時刻を共通制御フレームで送信すればよい。

【0061】

【発明の効果】以上の説明から理解できるように、本発明によれば、無線通信システムの基地局BSから複数種類の放送情報を同報チャンネルで送信しているため、無線端末あるいは移動端末の各ユーザに手軽で安価に放送情報を提供できる。また、本発明によれば、放送コンテンツ案内と放送時刻を予め放送しておき、各端末装置では、ユーザが予約した特定コンテンツの放送期間に選択的に受信回路を動作させ、受信した情報を蓄積するようにしているため、放送情報の入手に必要な受信動作期間を限定でき、電池の消耗を抑制することが可能となる。

【0062】本発明によれば、ユーザが予約した放送情報が、コンテンツ更新の都度、各端末内の記憶装置に自動的に蓄積され、ユーザからの要求に応じて出力できるようになっているため、各端末ユーザは、所望の放送情報を自分に都合の良いタイミングで参照できる。また、各端末は、一般通話チャンネルを介して情報サービスシステムと自動的に交信して、暗号解読キーを入手するための通信手順実行機能をもたせることにより、有料放送情報を暗号化して放送することが可能となる。この場合、上記通信手順の完了を契機として、解読キーの要求元ユーザに放送情報の課金処理を行うことにより、放送情報の使用料金を確実に回収することも可能になる。

【図面の簡単な説明】

【図1】本発明による放送情報配信システムの全体的な構成を示すブロック図。

【図2】基地局から送信される制御フレームのフォーマットの1例を示す図。

【図3】基地局から送信される同報フレームのフォーマットの1例を示す図。

【図4】上記同報フレームのヘッダ部の構成の1例を示す図。

【図5】本発明による放送情報配信システムの1実施例において、基地局と移動端末との間に形成される無線チャンネルの構成を示す図。

【図6】基地局の構成の1例を示すブロック図。

【図7】移動端末の構成の1例を示すブロック図。

【図8】基地局の送信回路の詳細を示すブロック図。

【図9】基地局の受信回路の詳細を示すブロック図。

【図10】移動端末で形成されるコンテンツ案内テーブルの構成を示す図。

【図11】移動端末で形成されるコンテンツ予約テーブルの構成を示す図。

【図12】本発明において、移動端末によって実行される放送情報を受信するためのプログラムの1実施例を示すフローチャート。

【図13】図12のプログラムにおける符号読取キー取得処理ルーチン150の詳細を示すフローチャート。

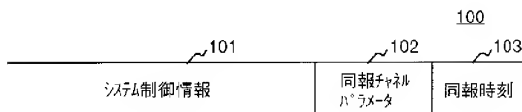
【図14】ユーザからのコンテンツ予約要求に応答して移動端末で実行されるプログラムの1実施例を示すフローチャート。

【図15】ユーザからの放送情報出力要求に応答して移動端末で実行されるプログラムの1実施例を示すフローチャート。

【符号の説明】

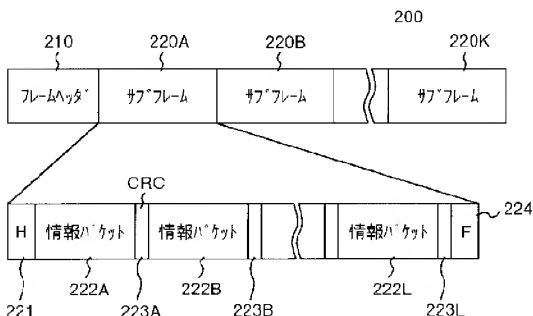
10：コンテンツ供給システム、20：通信プロバイダ、60：無線端末
100：制御フレーム、102：同期チャネルパラメータ、103：同報時刻、200：同報フレーム、210：フレームヘッダ、220：サブフレーム、400：コンテンツ案内テーブル、500：コンテンツ予約テーブル

【図2】



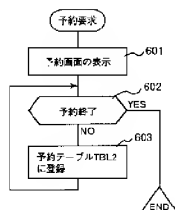
【図3】

図 3



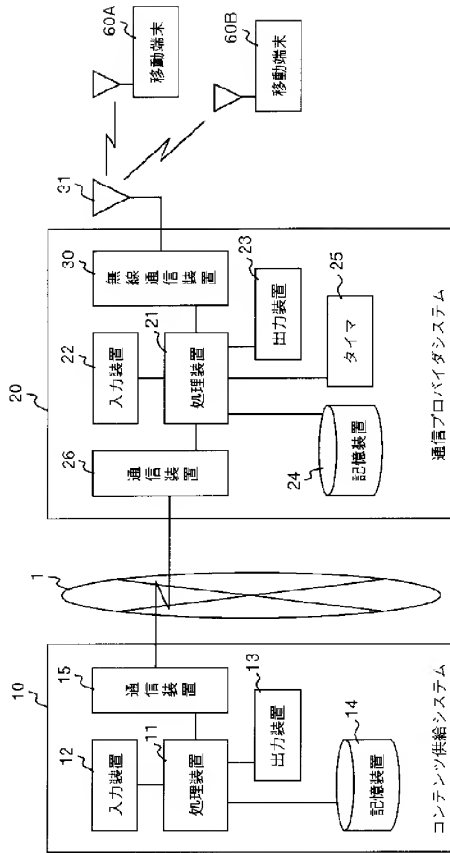
【図14】

図 14

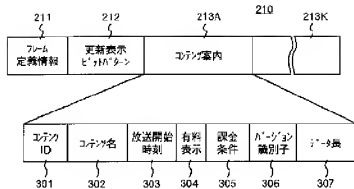


【図1】

図 1



【図 4】



【図 10】

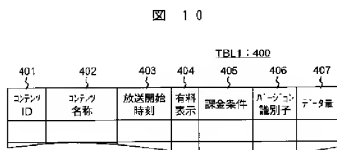
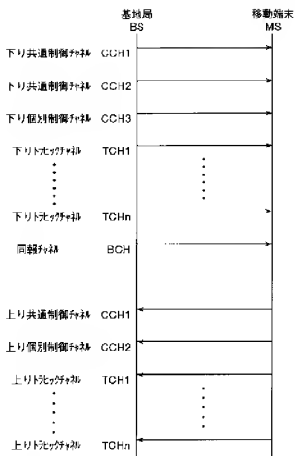


図 10

【図 5】



【図 6】

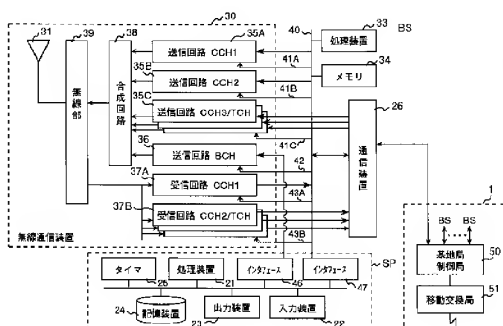


図 6

【図 11】

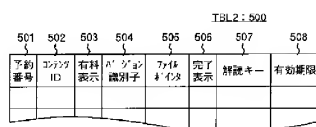
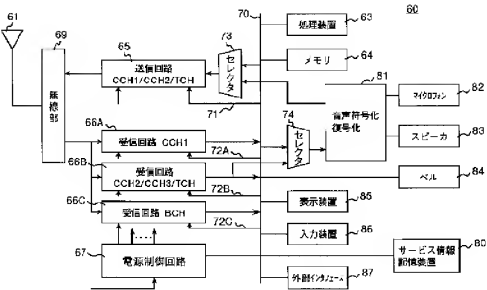


図 11

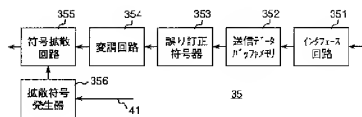
【図 7】

图 7



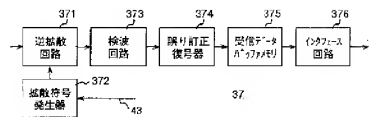
【图 8】

8



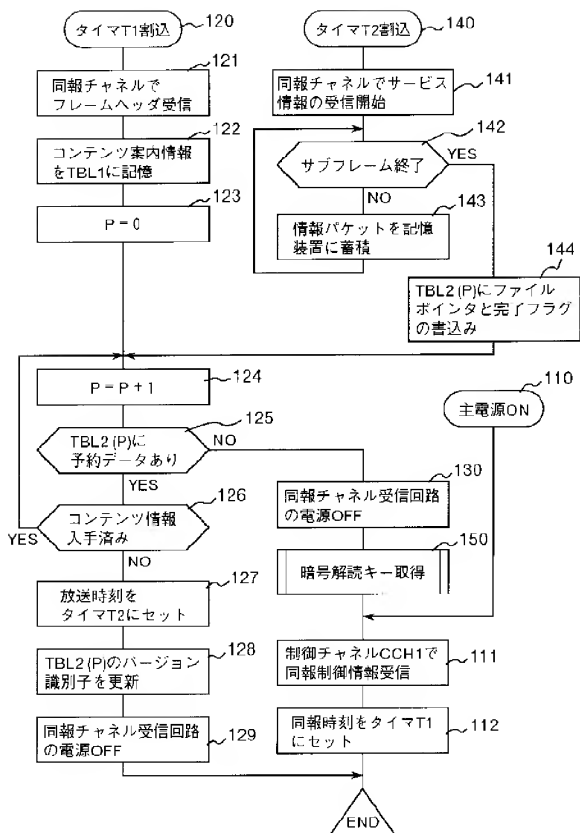
【図 9】

9



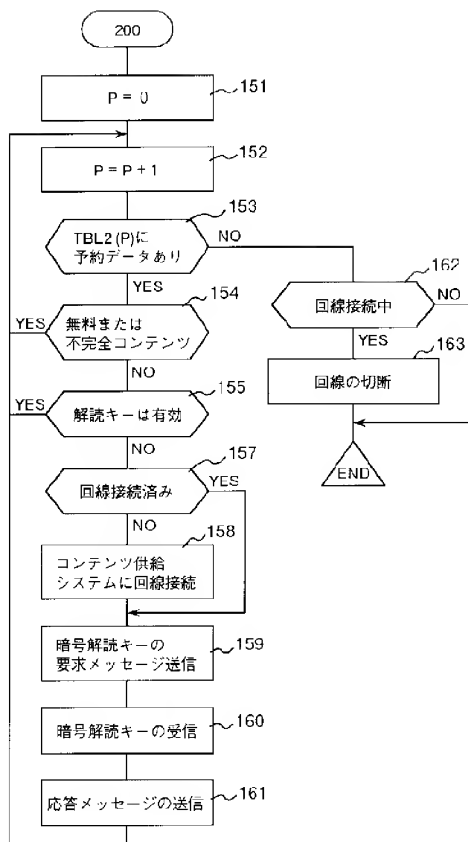
【図12】

図 12



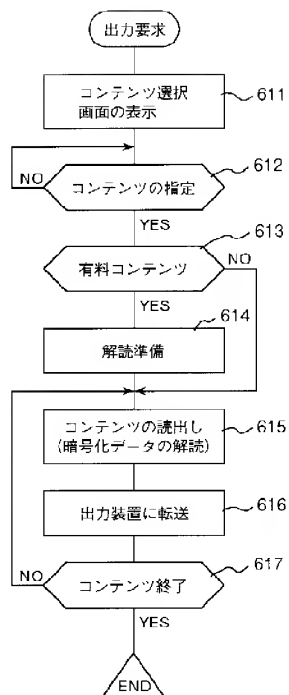
【図13】

図 13



【図15】

図 15



フロントページの続き

(51) Int. Cl.⁶

H 0 4 H 1/00

1/02

H 0 4 M 11/00

識別記号

3 0 3

F I

H 0 4 H 1/02

H 0 4 M 11/00

G 0 9 C 1/00

H 0 4 B 7/26

F

3 0 3

6 6 0 F

1 0 5 D

// G 0 9 C 1/00

6 6 0

1 0 9 M

JP11331150A

CERTIFYING/CHARGING METHOD FOR INFORMATION USER, METHOD FOR DISTRIBUTING INFORMATION FOR INFORMATION RESTORATION TO INFORMATION USER, RADIO CALLING DEVICE AND REPRODUCING OR RECEIVING DEVICE

Publication number : JP11331150A

Date of publication of application : 30.11.1999

Application number : 10-130274

Applicant : SONY CORP

Date of filing : 13.05.1998

Inventor : KORI TERUHIKO

Abstract:

PROBLEM TO BE SOLVED: To secure a communication means between a certifying/charging institution and a user through a simple method, in utilizing information.

SOLUTION: For this certifying/charging method, an information user reports personal information, including identification information for identifying the information user and information required for charging and identification information previously applied for specifying information or the information contents to be defined as a utilization object through a telephone line to the certifying/ charging institution. After the substance or client of utilization is specified based on this information, the certifying/charging institution distributes information for information restoration for every information defined as the utilization object to the information user through a radio call to that user. The information user cancels the enciphering applied to the utilization information, through the use of the received information for information restoration.

特開平11-331150

(43)公開日 平成11年(1999)11月30日

(51)Int.Cl. ⁶	識別記号	F I
H 0 4 L 9/32		H 0 4 L 9/00 6 7 3 A
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00 6 6 0 B
H 0 4 Q 7/38		H 0 4 H 1/02 F
H 0 4 H 1/02		H 0 4 B 7/26 1 0 9 S
H 0 4 Q 7/10		H 0 4 Q 7/02 B

審査請求 未請求 請求項の数14 ○L (全 10 頁) 最終頁に続く

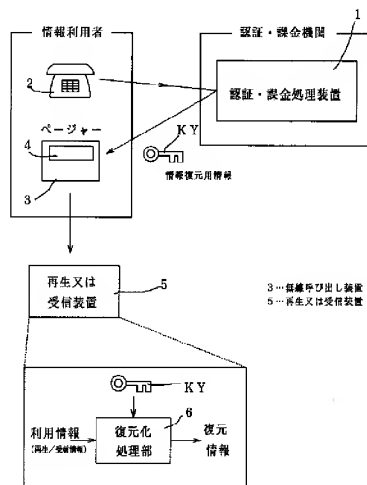
(21)出願番号	特願平10-130274	(71)出願人	000002185 ソニー株式会社 東京都品川区北品川 6 丁目 7 番35号
(22)出願日	平成10年(1998)5月13日	(72)発明者	郡 照彦 東京都品川区北品川 6 丁目 7 番35号 ソニー株式会社内
		(74)代理人	弁理士: 小松 祐治

(54)【発明の名称】 情報利用者についての認証・課金方法、情報利用者への情報復元情報の配布方法及び無線呼び

(57)【要約】 出し装置、並びに再生又は受信装置

【課題】 情報の利用にあたって、簡易な方法で認証・課金機関と利用者との間の通信手段を確保する。

【解決手段】 情報利用者を識別するための識別情報及び課金に必要な情報を含む個人情報と、利用対象とされる情報又は当該情報内容特定するために予め付与されている識別情報とを、情報利用者が電話回線を通して認証・課金機関に通知する。認証・課金機関はこれによって利用主体及び客体特定した後、情報利用者への無線呼び出しによって当該利用者に対してその利用対象とされる情報毎に情報復元情報を配布する。情報利用者は受信した情報復元情報を用いて利用情報に施された暗号化を解除する。



【特許請求の範囲】

【請求項1】 情報利用者の加入登録情報に基づいて利用料金を請求する認証・課金機関が、情報利用者の個人情報や利用状況情報を管理するための、情報利用者についての認証・課金方法において、

情報利用者を識別するための識別情報及び課金に必要な情報を含む個人情報と、利用対象とされる情報又は当該情報内容特定のために予め付与されている識別情報とを、情報利用者が電話回線を通して認証・課金機関に通知することによって、認証・課金機関が利用主体及び客体を特定することを特徴とする情報利用者についての認証・課金方法。

【請求項2】 請求項1に記載した情報利用者についての認証・課金方法において、情報利用者が、電話回線を通して認証・課金機関にパスワードを送出し、認証・課金機関が当該パスワードを、情報利用者について予め設定されているパスワードと照合することによって当該利用者の確認を行うことを特徴とする情報利用者についての認証・課金方法。

【請求項3】 情報利用者に対してその加入登録情報に基づいて利用料金を請求する認証・課金機関が、情報利用者への無線呼び出しによって当該利用者に対してその利用対象とされる情報毎に情報復元用情報を配布することを特徴とする情報利用者への情報復元用情報の配布方法。

【請求項4】 請求項3に記載した情報利用者への情報復元用情報の配布方法において、

(イ) 利用対象とされる情報毎に付与される情報復元用情報を、認証・課金機関と情報利用者との間で通する鍵情報を用いて認証・課金機関が暗号化した後、

(ロ) (イ)で暗号化された情報復元用情報を、認証・課金機関が情報利用者への無線呼び出しによって当該利用者へに通知し、

(ハ) (ロ)で通知された情報復元用情報に施された暗号化を、情報利用者が(イ)の鍵情報と同じ鍵情報を用いて解除することを特徴とする情報利用者への情報復元用情報の配布方法。

【請求項5】 請求項3に記載した方法に使用する無線呼び出し装置であって、

利用対象とされる情報又は当該情報内容特定のために予め付与されている識別情報及び利用対象とされる情報の情報復元用情報を、認証・課金機関から受信するとともに、これらの情報を文字情報として表示することを特徴とする無線呼び出し装置。

【請求項6】 請求項4に記載した方法に使用する無線呼び出し装置であって、

利用対象とされる情報又は当該情報内容特定のために予め付与されている識別情報及び暗号化された情報復元用情報を、認証・課金機関から受信するとともに、これらの情報を文字情報として表示することを特徴とする

無線呼び出し装置。

【請求項7】 請求項3に記載した方法に使用する無線呼び出し装置であって、利用対象とされる情報の再生又は受信を行う装置に対して、情報復元用情報を伝達するための送信手段を備えていることを特徴とする無線呼び出し装置。

【請求項8】 請求項4に記載した方法に使用する無線呼び出し装置において、

利用対象とされる情報の再生又は受信を行う装置に対して、情報復元用情報を伝達するための送信手段を備えていることを特徴とする無線呼び出し装置。

【請求項9】 請求項5に記載した無線呼び出し装置において、

利用対象とされる情報の再生又は受信を行う装置に対して、情報復元用情報を伝達するための送信手段を備えていることを特徴とする無線呼び出し装置。

【請求項10】 請求項6に記載した無線呼び出し装置において、

利用対象とされる情報の再生又は受信を行う装置に対して、情報復元用情報を伝達するための送信手段を備えていることを特徴とする無線呼び出し装置。

【請求項11】 請求項3に記載した方法に使用する再生又は受信装置であって、利用対象とされる情報の情報復元用情報が入力された場合に、当該情報に基づいて利用対象とされる情報の復元化処理を行うことを特徴とする再生又は受信装置。

【請求項12】 請求項4に記載した方法に使用する再生又は受信装置であって、暗号化された情報復元用情報が入力された場合に、該情報に施された暗号化を、予め設定されている鍵情報を用いて解除するとともに、当該情報に基づいて利用対象とされる情報の復元化処理を行うことを特徴とする再生又は受信装置。

【請求項13】 請求項11に記載した再生又は受信装置において、利用対象とされる情報について無線呼び出し装置で受信した情報復元用情報を装置内に取り込むための受信手段を備えていることを特徴とする再生又は受信装置。

【請求項14】 請求項12に記載した再生又は受信装置において、利用対象とされる情報について無線呼び出し装置で受信した情報復元用情報を装置内に取り込むための受信手段を備えていることを特徴とする再生又は受信装置。

【発明の詳細な説明】

【0000】

【発明の属する技術分野】本発明は、情報利用者についての認証・課金方法や情報利用者への情報復元用情報(暗号解読鍵等)の配布方法に関するものである。

【0002】

【従来の技術】デジタル化された音声情報や映像情報

等の再生や受信において、従来の方法では再生装置や受信装置の利用者の認証・課金について専用の情報記録媒体や装置を用いる必要がある。

【0003】例えば、デジタル衛星放送受信機では、専用のICカードを用いて受信機と認証・課金機関（あるいはセンター）との間の電話回線を通して利用者の個人情報や利用の許可情報、利用状況の情報を管理している。つまり、受信機には利用者認証・課金機関との間の通信を行うための通信手段としてモデム（変復調器）が内蔵されており、モデム接続によって電話回線を通して利用者から認証・課金機関に対して個人情報や利用状況の情報が通知され、また、認証・課金機関から利用者には情報利用の許可情報が通知される。

【0004】

【発明が解決しようとする課題】しかしながら、従来の認証・課金機関と利用者との間の通信手段に関して下記に示すような問題点がある。

- 【0005】（a）通信設備が大掛かりである
- （b）装置の設置場所が制限される
- （c）パッケージメディアの再生装置への適用が困難である
- （d）利用者について個人の特定が困難である
- （e）通信費用の低減が困難である。

【0006】先ず、上記（a）については、装置のコスト上昇を招いたり、接続工事が必要になる。例えば、上記したデジタル衛星放送受信機では装置内に内蔵モデムが必要であり、また、モデムを電話回線に接続するための工事が必要となる。

【0007】そして、（b）については、例えば、家庭内で受信機の内蔵モデムを電話回線に接続することのできる場所が限られている場合において、受信機の設置場所と受信情報の利用場所とが離れていると機器の接続作業が面倒である。

【0008】（c）については、光ディスク（例えば、コンパクトディスク（CD）やミニディスク（MD）等。）等のパッケージメディアの再生装置に対してその内蔵モデムの接続という新たな工事を利用者に要求することは許容され難い。

【0009】（d）については、情報提供に対する課金を、電話番号に基づいて行う方法では、真の利用者である個人を特定することが困難である場合が多い（例えば、家族全員で一つの電話を共用している場合等。）。

【0010】（e）については、利用者個人の特定という点に関して携帯電話やPHS（Personal Handy phone System）では個人での使用比率が高いので、これらを利用する方法が考えられるが、通信費用が高いので少額の課金には不向きである。

【0011】そこで、本発明は、情報の利用にあたって、簡易な方法で認証・課金機関と利用者との間の通信手段を確保することを課題とする。

【0012】

【課題を解決するための手段】本発明は上記した課題を解決するために、情報利用者を識別するための識別情報及び課金に必要な情報を含む個人情報と、利用対象とされる情報又は当該情報内容を特定するために予め付与されている識別情報とを、情報利用者が電話回線を通して認証・課金機関に通知することによって、認証・課金機関が利用主体及び客体を特定する方法と、認証・課金機関が、情報利用者への無線呼び出しによって当該利用者に対してその利用対象とされる情報毎に情報復元用情報（暗号解読鍵等）を配布する方法とを提案するものである。

【0013】従って、本発明によれば、認証・課金機関と情報利用者とは、電話回線と無線呼び出しという簡易な通信方法によって結び付けることが可能となる。

【0014】

【発明の実施の形態】図1は、本発明に係る概要の説明図であり、情報利用者についての認証・課金方法及び当該利用者への情報復元用情報の配布方法について示すものである。

【0015】尚、ここでいう「情報」には、音声情報や映像情報等の情報や、コンピュータ機器で使用する情報等、一切の情報が含まれ、デジタル情報、アナログ情報の如何は問わない。また、本発明に関する限り情報利用者への情報の伝達形態が特定されることはなく、光ディスク等の情報記録媒体から再生される情報や、有線又は無線通信（コンピュータネットワークや衛星通信等。）を通して受信される情報等、各種の情報に利用することができる。

【0016】図1において、主体は情報利用者と、認証・課金機関である。

【0017】認証・課金機関は、情報利用者の加入登録情報に基づいて当該利用者に利用料金を請求する機関であり、認証・課金処理装置1を有する。

【0018】情報利用者から認証・課金機関への通信接続（アップリンク）には、電話回線が用いられ、情報利用者は、所望の情報を利用するために先立って、下記に示す情報を電話2で認証・課金機関に通知する。

【0019】（I）情報利用者を識別するための識別情報及び課金に必要な情報を含む個人情報

（II）利用対象とされる情報又は当該情報内容を特定するために予め付与されている識別情報。

【0020】先ず、（I）の情報は、情報利用者を特定するために必要であり、個人情報には、氏名、住所、電話番号等の他、クレジットカード番号、利用金融機関や口座番号等が含まれる。

【0021】また、（II）の情報は、情報利用者が利用を意図している情報を特定するために必要な情報であり、例えば、情報記録媒体に付された識別番号、番組情報やプログラム番号、タイトルID等が挙げられる。

【0022】認証・課金機関はこれらの情報について、例えば、（音声）電話回線を介してトーン信号や無線呼び出しによる文字情報等で情報利用者から通知を受けることで、利用主体及び客体を特定する。

【0023】尚、個人情報漏洩等に起因する損害の発生を防ぐためには、情報利用者の本人確認のためにパスワード（暗証番号や暗号コード等の暗号情報。）を要求することがセキュリティを高める上で望ましい。

【0024】即ち、情報利用者が上記した情報（Ⅰ）、（ⅠⅠ）に加えてパスワードを認証・課金機関に通知すると、該認証・課金機関は当該パスワードを、情報利用者について予め設定されているパスワードと照合することによって当該利用者の本人確認を行う。

【0025】認証・課金機関は、上記（Ⅰ）の情報から作成される加入登録情報に基づいて、上記（ⅠⅠ）の情報の利用に対する課金情報を集計した後、情報利用者への代金支払い請求・集金を行う。尚、図では、説明の便宜上、認証・課金機関を一の機関としているが、認証機関と課金・徴収機関とを分離しても良いことは勿論である。また、徴収した金額から、著作権者に使用料が還元されることは勿論である。

【0026】不正な情報の取得、複製等を防止するためには、利用対象である情報に暗号化処理を施したり、スクランブル処理（伝送情報の盗聴等を防止するために情報を攪乱させる処理）等を行うことが効果的であり、そのためには、認証・課金機関が正式に認知した情報利用者に対してのみが正規の情報提供サービスを受けられるようにすることが好ましい。

【0027】つまり、情報利用者に対してその加入登録情報に基づいて利用料金を請求する認証・課金機関が、情報利用者への無線呼び出しによって当該利用者に対してその利用対象とされる情報毎に情報復元用情報（暗号解読用の鍵情報等であり、図には鍵の図形で示す。）を配布する。

【0028】例えば、情報利用者が無線呼び出し装置3としてのページャー機（所謂ポケットベル）を所持しており、認証・課金機関から該情報利用者への通信（ダウンリンク）において、ページャー機を呼び出して情報復元用情報（これを「KY」と記す。）を通知する。尚、その際、利用対象とされる情報の識別情報も併せて通知されることは勿論である。例えば、ページャー機は、文字や図形情報を表示するための表示手段4を有しているので、上記情報（ⅠⅠ）及び情報復元用情報を、認証・課金機関から受信した際に、これらの情報が文字情報として表示される。

【0029】正規に加入登録した情報利用者は、情報復元用情報（KY）を再生又は受信装置5に入力することによって、利用を意図する情報に施された暗号化等の秘匿処理を解除して、意味ある情報を取り出すことができる。つまり、情報の再生又は受信装置5内には、再生情報

又は受信情報の復号化等を行うための復元化処理部6が設けられており、該復元化処理部6は、情報復元用情報（KY）を用いて情報を復元（暗号化の解除等。）し、情報利用者による直接の利用が可能な形態に変換する。

【0030】尚、無線呼び出しによって情報利用者に通知される情報復元用情報の漏洩や盗聴等を未然に防止するためには、情報復元用情報に対して暗号化を施しておく、この暗号化された情報復元用情報を再生又は受信装置5に入力したときに、当該情報に施された暗号化を、予め設定されている鍵情報を用いて解除するとともに、解除後の情報復元用情報に基づいて、利用対象である情報の復元化処理を行うことが望ましい。

【0031】つまり、この場合には、下記に示す（i）乃至（i i i）の手順を採る。

【0032】（i）利用対象とされる情報毎に付与される情報復元用情報を、認証・課金機関と情報利用者との間で適用する鍵情報を用いて認証・課金機関が暗号化する

（i i）（i）で暗号化された情報復元用情報を、認証・課金機関が情報利用者への無線呼び出しによって当該利用者へ通知する

（i i i）（i i）で通知された情報復元用情報に施された暗号化を、情報利用者が（i）の鍵情報と同じ鍵情報を用いて解除する。

【0033】例えば、図2に示すように、情報復元用情報を鍵情報「A」とする場合において、これを鍵情報「B」によって暗号化する（図には、鍵情報Aを箱詰めにした後、これに付する錠前Lに鍵情報Bで鍵をかけた状態の図で概念的に示す。）。

【0034】この作業は認証・課金機関によって行われ、秘匿化された鍵情報Aが情報利用者のページャー機に通知される。例えば、暗号化された鍵情報Aがページャー機に文字情報として表示される。

【0035】情報利用者は、事前に所有している鍵情報Bを使って鍵情報Aの暗号化を解除してこれを取り出す（図には、箱詰めにした鍵情報Aに付設された錠前Lを鍵情報Bで外した状態の図で概念的に示す。）。

【0036】そして、この鍵情報Aを使って利用対象である情報「HⅠ」に施された暗号化を解除する（図には、箱詰めにした情報HⅠに付設された錠前Mを鍵情報Aで外した状態の図で概念的に示す。）。これによって、情報利用者には意味ある情報の利用が可能になる。このように、利用対象である情報及びその情報復元用情報の両者に対して秘匿処理を施すことによって2重の安全対策を講じることができる。

【0037】本発明に使用する無線呼び出し装置においては、図3に示すように、情報復元用情報（KY）を情報の再生又は受信装置5に伝送するための送信手段7を設けることが好ましい。即ち、情報復元用情報を再生又は受信装置5に伝送する方法には、再生又は受信装置に

操作入力部を付設して、キー操作入力によって手動で情報復元用情報を入力する方法があるが、無線呼び出し装置 3 に送信手段 7 を設けるとともに、再生又は受信装置 5 には、情報復元用情報を装置内に取り込むための受信手段 8 を設けることで、キー入力の手間を省くことができる。尚、図では、無線呼び出し装置 3 内の受信部 9 で受信した情報復元用情報（KY）を表示手段 4 に送出して表示するとともに、送信手段 7 から再生又は受信装置 5 の受信手段 8 を介して復元処理部 6 に情報復元用情報が送信される。

【0038】また、送信手段 7 から受信手段 8 への情報の伝送形態については有線方式又は無線方式（赤外線や微弱電波等の電磁波、音声、超音波等を用いる。）が挙げられるが、後者の方が便利である。この他、図 4 に示すように、無線呼び出し装置 3 を再生又は受信装置 5 に装着して情報を受け渡す方法の場合には、カードバス等のインターフェース部を用いた端子接続（無線呼び出し装置 3 に設けられた送信側の端子部 7 A と、再生又は受信装置 5 に設けられた受信側の端子部 8 A とを接続する。）によって情報を直接的に取り出せるので、無線呼び出し装置 3 をあたかも IC カードのように取り扱うことができる。

【0039】

【実施例】図 5 及び図 6 は光学読取式の情報記録媒体（例えば、コンパクトディスクやミニディスク等の光ディスク）を用いたパッケージメディアの再生システムに本発明を適用した実施の一例を示すものである。尚、本発明に関する限り、情報記録媒体についての形態の如何は問わないので、ディスク状に限らず、テープ状、シート状、カード状等、各種の媒体に幅広く適用することができることは勿論である。

【0040】図 5 は認証・課金システムと光ディスクの再生装置を示すものであり、光ディスク 10 の記録情報については鍵情報「A」によって暗号化が施されている（図には、光ディスクそのものに付した錠前 M に鍵情報 A で鍵をかけた状態の図で概念的に示す。）。よって、該光ディスクの記録内容を取り出すのに通常の再生動作では不十分であり、暗号化の解除を必要とする。

【0041】この光ディスク 10 を入手したユーザー（情報利用者）は、まず、認証・課金センターに電話をかける。

【0042】認証・課金センターでは、例えば、自動応答システムが導入された処理装置を用いて音声ガイドが行われ、ユーザーはガイド音声に従ってプッシュ紐を操作し、これによって発生するトーン信号によって、必要な情報を認証・課金センターに通知する。尚、ここで必要な情報とは、ポケットベル番号、暗証番号、光ディスク又はコンテンツ（情報内容）に固有の識別情報（ID 番号）等である。

【0043】認証・課金センターは、まず、通知された

ポケットベル番号及び暗証番号に基づいて相手が正規に登録済のユーザーであるか否かを判断する。そして、正規登録ユーザーの確認がとれた場合に、当該ユーザーに対して光ディスクやコンテンツに固有の識別情報を要求する。ユーザーは要求された識別情報を入力し、これを受けて認証・課金センターは、当該識別情報に対応した鍵情報（この場合は、鍵情報 A）を、別の鍵情報「B」（ユーザーと認証・課金センターとの間で予め定められている。）を使って暗号化（図 5 の錠前 L 参照。）した後、これをユーザーの所有するポケットベル 11 に送信する。尚、ポケットベルは小型軽量の個人携帯端末であるため、特に携帯用の再生装置への適用（再生装置と組みにした使用）が容易であり、また、サービスエリアが広いため基地局の設置や維持に必要な費用が少なくて済むといった利点がある。

【0044】認証・課金センターでは、その後、暗号化された鍵情報 A の送信が完了した時点で、ポケットベル番号に対応する加入登録情報に従って課金・徴収処理を行う。つまり、暗号化された鍵情報 A の発行時点での課金が可能であり、これによって利用料金の徴収についての確実性を高めることができる。

【0045】このように暗号化された鍵情報 A はユーザーのポケットベル 11 で着信されるが、当該情報を再生装置 12 に入力し又は転送する方法には、例えば、下記の（1）乃至（4）に示す方法が挙げられる。

【0046】（1）ポケットベルの表示部（液晶ディスプレイ等）に文字表示される鍵情報を見て、ユーザーがキー操作で再生装置に入力する方法

（2）ポケットベルに設けられたカードインターフェースによって、ポケットベル本体を再生装置に装着して鍵情報を転送する方法

（3）ポケットベルに付設された通信用の発光部（発光ダイオード等）によって赤外線を発して、これを再生装置の受光部（フォトダイオード等）で受光することで鍵情報を転送する方法

（4）ポケットベルに付設された発信部によって微弱な電波を発信し、これを再生装置の受信部で受け取ることによって鍵情報を転送する方法

【0047】こうして再生装置に伝送された鍵情報 A は、予め装置内に用意されている鍵情報 B を使って復号化される（錠前 L が外される。）。そして、この復号化された鍵情報 A によって、光ディスク 10 の記録情報に施された暗号化が解除（復号化）されて（錠前 M が外される。）、情報の再生が可能となる。

【0048】図 6 は以上の手順を時間の順序に従ってまとめたものであり、下記（1）乃至（5）に示す通りである。

【0049】（1）ポケットベル番号・暗証番号の通知

（2）コンテンツ ID（識別情報）の要求

（3）コンテンツ ID の通知

(4) 鍵情報Aの送信

(5) 鍵情報の受信確認

尚、奇数番号で示す手続がユーザーから認証・課金センターに対して行われ、偶数番号で示す手続が認証・課金センターからユーザーに対して行われる。

【0050】図7は、本発明をデジタル衛星放送におけるユーザー認証・課金方法及びシステムに適用した実施の一例を示すものである。

【0051】放送業者と認証・課金センターとは専用回線で結ばれており、放送業者は放送衛星を介して、ユーザーの使用する受信装置1.3に情報を送信する。

【0052】ユーザーと認証・課金センターとの間の通信については、電話回線及び無線呼び出しによって上記した説明と同様に行う。即ち、上記の説明において、「光ディスクの記録情報」を「受信を意図する情報（番組情報等）」とし、また、鍵情報Aによる情報の「暗号化」を「暗号化あるいはスクランブル処理」とする等の読み替えを適宜に行えば良い。要するに、この場合にはユーザーの認証及びコンテンツの識別情報の通知が電話回線を介して認証・課金センターに行われた後、該センターからユーザーに対してコンテンツの利用を許可するための情報（スクランブル処理の解除（デスクランブル）用情報等）又は当該情報を鍵情報Bで暗号化した情報をユーザー所有のポケットベル1.1に通知される。

【0053】デジタル衛星を利用した従来のシステムでは、受信装置にモデム等の通信手段を設けて当該受信装置と認証・課金センターの処理装置との間を電話回線で接続する必要があるが、本発明ではこのような通信手段を受信装置に設ける必要がないので、受信装置の設置場所が制限されることはない。

【0054】また、従来のシステムではユーザーの個人情報や許可情報、利用状況の情報等を格納する専用カード（ICカード）を受信装置に装着する必要があるが、上記のように、個人用携帯端末であるポケットベルを、ユーザー個人の認証・課金用のカードとして代用することによって認証・課金センターとの通信手段を容易に確保することができる。しかも、ポケットベルは、比較的安価に利用することができ普及率も高いので少額課金のシステムへの利用にとって有利であり、利用料金の徴収時にも活用することができる。そして、ポケットベルは、他の携帯端末に比して個人の使用比率が高く、また、契約しない并使用できない携帯端末であるため、個人の特長が容易である。

【0055】図8はインターネットを利用してコンピュータ機器に音楽情報を配布するシステムに本発明を適用した例を示すものである。

【0056】ユーザーは、まず、コンピュータ（PC）及びモデム等の通信手段を使ってインターネット経由で情報提供機関の会員データベースにアクセスし、自分のID（識別）番号及びパスワードを入力する。

【0057】ユーザーの認証が済むと、ユーザーはWWW（World Wide Web）ブラウザ（閲覧ソフト）を使って自分の意図する音楽ソフトの配信を情報提供機関に依頼する。

【0058】これを受けて情報提供機関は、配信サーバを用いて、コンテンツ・データベースに格納されている音楽ソフトの中からユーザーから依頼されたものを検索して取り出し、これに暗号化及び電子透かしを施した情報（図には、音符記号で示す音楽ソフトを箱詰めにした上でその錠前Mに鍵情報「A」で鍵をかけた状態の図で概念的に示す。）をインターネット経由でユーザーのコンピュータ（PC）に送信することでダウンロードが完了する。尚、「電子透かし」とは音声情報を録音中に耳では聞えないように情報を重畳して埋め込む方式（スペクトラム拡散等）を利用する。）であり、本例ではコンテンツ（この場合は音楽情報）の識別情報に対して用いている。

【0059】ユーザーは、ダウンロードした情報をそのままでは利用することができないので、音楽ソフトに施された電子透かしからコンテンツの識別情報を再生してこれを知り、情報提供機関に電話をかけて認証・課金に必要な情報及びコンテンツの識別情報を通知する。

【0060】情報提供機関からはユーザーのポケットベル1.1に、上記鍵情報Aを別の鍵情報「B」で暗号化した情報（図には、鍵情報Aを箱詰めにした上でその錠前Lに鍵情報Bで鍵をかけた状態の図で概念的に示す。）が通知されるので、ユーザーは当該情報をコンピュータ（PC）に入力する。これによって事前に用意されている鍵情報Bを使って鍵情報Aの復号化を行う。

【0061】こうして、元の鍵情報Aが得られるので、これを使って音楽ソフトの復号化を行うことができる。

【0062】尚、鍵情報Aや音楽ソフトの復号化処理は、コンピュータ（PC）上でソフトウェア処理により実現される専用プレーヤ（音楽再生用ソフトウェア）で行われ、ここでは鍵情報Aで暗号化された音楽ソフトが鍵情報Aで暗号化されたファイルとして取り扱われ、ユーザーが鍵情報Bで暗号化された鍵情報Aを入力すると、鍵情報Aの復号化、これに続く音楽ソフトの復号化が行われて音楽ソフトの再生が可能となる。また、ユーザーが音楽ソフトを受け取る経路と、暗号化された鍵情報を受け取る経路とを分けることによって安全性を高めることができる。

【0063】しかして、本発明によれば、情報の配布形態の如何に関係なくユーザーの認証・コンテンツに係る課金システムに幅広く適用することができる。

【0064】また、同一のコンテンツであっても、該コンテンツのID（識別情報）毎に暗号鍵を変えることによってセキュリティ面の強化が可能であり、また、加入登録者又は使用する機器毎に鍵情報Bを変えたり、あるいはこれを時間の経過に伴って更新していく方法によ

り、さらに高いセキュリティを維持することができる。

【0065】

【発明の効果】以上に記載したところから明らかなように、請求項1に係る発明によれば、電話回線を通して必要な情報を認証・課金機関に通知することで、認証・課金機関が利用主体及び客体を特定することができるので、通信設備が大掛かりにならず、また、使用装置の設置場所が制限されない。また、パッケージメディアの再生装置への適用、利用者個人の特定等が容易である。

【0066】請求項2に係る発明によれば、情報利用者が電話回線を通して認証・課金機関にパスワードを送出して認証・課金機関により情報利用者の確認が行われるので、他人による不正な利用を防止することができる。

【0067】請求項3に係る発明によれば、認証・課金機関が、情報利用者への無線呼び出しによって当該利用者個人を特定して情報復元用情報を配布することができる、また通信費用の低減や通信設備の簡易化を図るとともに、装置の使用場所についての制約を排除することができる。

【0068】請求項4に係る発明によれば、情報復元用情報に対して暗号化を施すことによって当該情報の配布時の漏洩に起因する損害の発生を防止することができる。

【0069】請求項5、6に係る発明によれば、認証・課金機関から受信した識別情報や情報復元用情報を文字情報として表示することによって、これらの情報を情報利用者が直ちに認識して利用することができる。

【0070】請求項7乃至10に係る発明によれば、情報の再生又は受信を行う装置に対して、情報復元用情報を送信手段によって伝達することで、当該装置への情報の入力を容易に行うことができる。

【0071】請求項11に係る発明によれば、情報復元用情報の入力機能や情報の復元化機能を有する装置での

み有意义的情報の利用が可能となるので、不正な情報利用の可能性を排除することができる。

【0072】請求項12に係る発明によれば、利用対象情報及び情報復元用情報に対して暗号化を施すことによって2重の安全対策を講じることができる。

【0073】請求項13、14に係る発明によれば、無線呼び出し装置から情報復元用情報を容易に取り込むことができる。

【図面の簡単な説明】

【図1】本発明に係る概要の説明図である。

【図2】情報復元用情報の暗号化・復号化と情報復元用情報による秘匿情報の復元についての説明図である。

【図3】無線呼び出し装置から再生又は受信装置への通信形態について説明するための概略図である。

【図4】無線呼び出し装置と再生又は受信装置との端子接続による通信形態について説明するための概略図である。

【図5】図6とともに、光学読取式の情報記録媒体を用いたパッケージメディアの再生システムに本発明を適用した実施の一例を示すものであり、本図は認証・課金システム及び光ディスクの再生装置についての説明図である。

【図6】処理手順を時間経過に沿って示す説明図である。

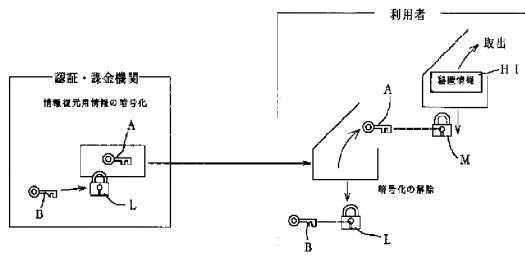
【図7】本発明をデジタル衛星放送におけるユーザー認証・課金方法及びシステムに適用した実施の一例を示す図である。

【図8】インターネットを利用してコンピュータ機器に音楽情報を配布するシステムに本発明を適用した実施の一例を示す図である。

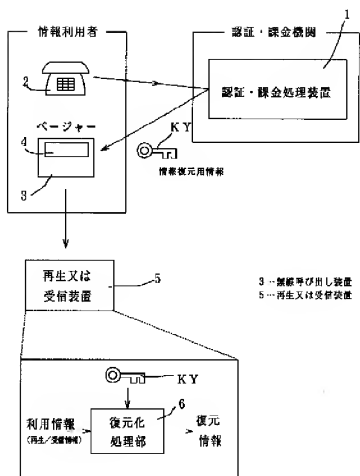
【符号の説明】

3…無線呼び出し装置、5…再生又は受信装置、7、7A…送信手段、8、8A…受信手段

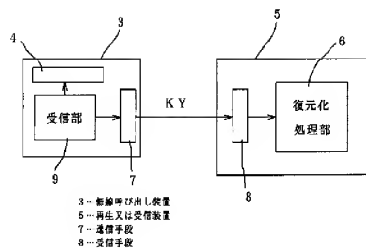
【図2】



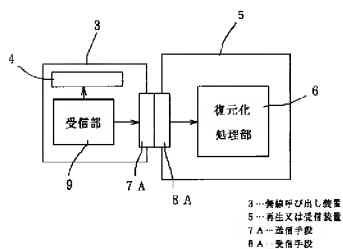
【図1】



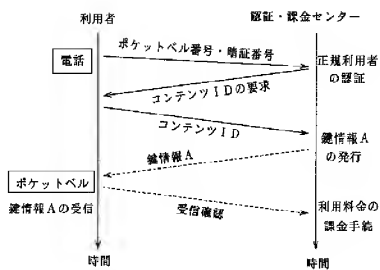
【図3】



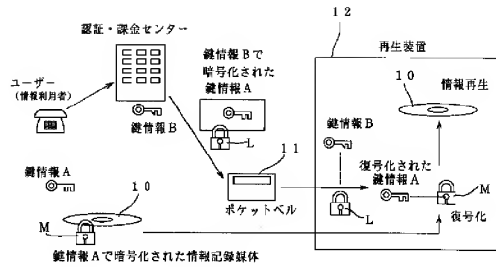
【図4】



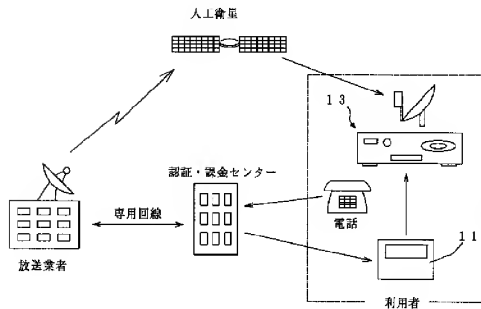
【図6】

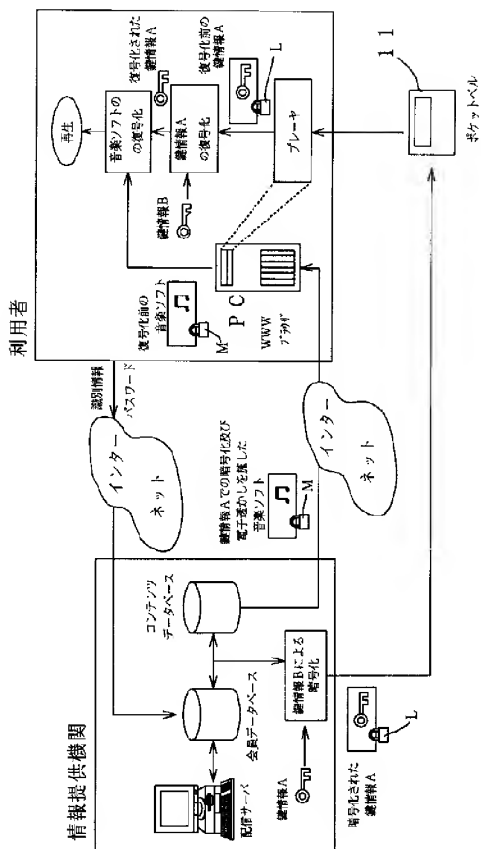


【図 5】



【図 7】





フロントページの続き

(51) Int. Cl. ⁶

H O 4 Q 7/20

識別記号

F I

H O 4 Q 7/04

D

JP11355460A

CONNECTION METHOD FOR ISDN LINE

Publication number : JP11355460A

Date of publication of application : 24.12.1999

Application number : 10-154057 Applicant : MEIDENSHA CORP

Date of filing : 03.06.1998 Inventor : NISHIBE YASUNORI

Abstract:

PROBLEM TO BE SOLVED: To restore a line that is tentatively interrupted due to an error.

SOLUTION: An ISDN connection device transmits 'normal interruption' as reason indication information of an interruption message on occurrence of channel interruption. A terminal server records its telephone number at the time of connection between the ISDN connection device and the channel. In the case that no 'normal interruption' is included in the received interruption message (S1), the restoration of the channel is awaited for a time of a channel restoration timer (S2, S7), and then a connection message with respect to the channel is received (S3). If the telephone number is coincident (S4), the channel is connected (S5), but in the case of dissidence, the acceptance of an incoming call is rejected (S6).

特開平11-355460

(43)公開日 平成11年(1999)12月24日

(51)Int.Cl.⁶ 識別記号
H 0 4 M 11/00 3 0 3
H 0 4 L 12/02
H 0 4 M 3/42

F I
H 0 4 M 11/00 3 0 3
3/42 E
H 0 4 L 11/02 Z

審査請求 未請求 請求項の数4 O L (全 7 頁)

(21)出願番号 特願平10-154057

(22)出願日 平成10年(1998)6月3日

(71)出願人 000006105

株式会社明電舎
東京都品川区大崎2丁目1番17号

(72)発明者 西部 保則

東京都品川区大崎2丁目1番17号 株式会
社明電舎内

(74)代理人 弁理士 志賀 富士弥 (外1名)

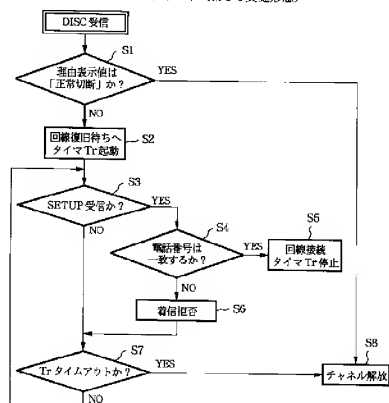
(54)【発明の名称】 I S D N回線の接続方法

(57)【要約】

【課題】 I S D N接続機器からI S D N交換機を介してI S D Nターミナルサーバに接続メッセージを送送してチャンネル接続し、切断メッセージを送送してチャンネルを解放する回線接続方法において、回線ケーブル障害等の異常には回線復旧ができなくなる場合がある。

【解決手段】 I S D N接続機器は、チャンネル切断時に切断メッセージの理由表示情報として「正常切断」を送送し、ターミナルサーバは、I S D N接続機器とのチャンネル接続時にその電話番号を記録しておき、受信した切断メッセージに「正常切断」が含まれないとき (S 1)、回線復旧タイマの時間だけ当該チャンネルを復旧待ち状態とし (S 2、S 7)、このチャンネルに対する接続メッセージの受信し (S 3)、電話番号が一致するとき (S 4)、回線接続し (S 5)、一致しないとき着信拒否する (S 6)。

フローチャート (第1の実施形態)



【特許請求の範囲】

【請求項1】 ISDN接続機器からISDN交換機を介してISDNターミナルサーバに接続メッセージを送信してチャネル接続し、切断メッセージを送信してチャネルを解放するISDN回線の接続方法において、前記ISDN接続機器は、チャネル切断時に前記切断メッセージの理由表示情報として「正常切断」を送信し、前記ターミナルサーバは、前記ISDN接続機器とのチャネル接続時にその電話番号を記録しており、前記ターミナルサーバは、受信した前記切断メッセージに前記「正常切断」が含まれないときに回線復旧タイムの時間だけ当該チャネルを復旧待ち状態とし、このチャネルに対する前記接続メッセージの受信時に前記電話番号が一致するときにチャネル接続を許可することを特徴とするISDN回線の接続方法。

【請求項2】 ISDN接続機器からISDN交換機を介してISDNターミナルサーバに接続メッセージを送信してチャネル接続し、切断メッセージを送信してチャネルを解放するISDN回線の接続方法において、前記ターミナルサーバは、前記ISDN接続機器とのチャネル接続時にその電話番号を記録しており、前記ターミナルサーバは、受信した前記切断メッセージの生成源がISDN接続機器でないときに回線復旧タイムの時間だけ当該チャネルを復旧待ち状態とし、このチャネルに対する前記接続メッセージの受信時に前記電話番号が一致するときにチャネル接続を許可することを特徴とするISDN回線の接続方法。

【請求項3】 ISDN接続機器からISDN交換機を介してISDNターミナルサーバに接続メッセージを送信してチャネル接続し、切断メッセージを送信してチャネルを解放するISDN回線の接続方法において、前記ISDN接続機器は、チャネル切断時に前記切断メッセージにユーザ・ユーザ情報要素を付加して伝送し、前記ターミナルサーバは、前記ISDN接続機器とのチャネル接続時にその電話番号を記録しており、前記ターミナルサーバは、受信した前記切断メッセージに前記ユーザ・ユーザ情報が含まれないときに回線復旧タイムの時間だけ当該チャネルを復旧待ち状態とし、このチャネルに対する前記接続メッセージの受信時に前記電話番号が一致するときにチャネル接続を許可することを特徴とするISDN回線の接続方法。

【請求項4】 前記ISDN接続機器は、ユーザ・ユーザ情報として通常接続要求と回線復旧要求の識別コードを付加して伝送し、前記ターミナルサーバは、当該チャネルの復旧待ち状態で前記ユーザ・ユーザ情報が回線復旧要求の場合にチャネル接続を許可することを特徴とする請求項1乃至3のいずれかに記載のISDN回線の接続方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ISDN接続機器とISDNターミナルサーバとの間のISDN回線の接続方法に係り、特にISDN回線異常時の復旧方法に関する。

【0002】

【従来の技術】インターネットの爆発的な普及にともなう、ISDN（サービス総合ディジタル網）を媒介としたコンピュータ等のISDN接続機器（以下、PCと呼ぶ）とLAN（ローカルエリアネットワーク）との間を接続するシステムの増加が目立ってきた。

【0003】このシステム構成は、図11に示すように、ユーザ側の各PC1₁～1_NはISDN公衆網交換機2を介してISDNターミナルサーバ（以下、TSと呼ぶ）3とのISDN回線接続を行い、接続したチャネルを通して、LANのデータを伝送する。

【0004】これにより、ユーザは、ISDN接続機器になるPC1₁～1_Nを遠方にあるLANにあたかも直接接続されているかのように操作することができる。ISDN回線は、所要の通信が終了し次第切断する。

【0005】

【発明が解決しようとする課題】通常、ISDNターミナルサーバ側の収容回線数は、接続できるPCの総数を満たさないのが普通である。したがって、回線の使用状況によっては、当然接続できないPCも存在する。

【0006】さて、ISDN回線を接続し、LANのデータ伝送を行っている最中に、PC1₁～1_NとISDN交換機2との間で一時的なケーブル障害などの回線異常が発生し、チャネルが切断されてしまった場合、PC1₁～1_Nはその異常を検出すると、自動的に回線の再接続を行い、LANへの伝送を再開しようとする。

【0007】ISDN交換機2とTS3間の回線は、しかるべき切断理由を含んだ切断メッセージがISDN交換機より発せられて、自動的に回線の切断が行われ、TSの該当するチャネルは空き状態となる。

【0008】このとき、TS3の該当するチャネル以外の全てのチャネルが使用状態にあり、かつ、該当するチャネルに対してもチャネルが空き状態となった直後に、別のPCから接続が行われてしまった場合、回線異常が発生したPCは、もはや回線を復旧させることができなくなり、データ伝送の途中でネットワーク異常となってしまう。

【0009】本発明の目的は、回線異常で回線が一時的に切断されたときの回線復旧を可能にしたISDN回線の接続方法を提供することにある。

【0010】

【課題を解決するための手段】本発明は、ISDNターミナルサーバ側において、切断メッセージに含まれる切断理由や切断要求の生成源又はユーザ・ユーザ情報の有無により正規の切断要求か回線異常による切断要求かを判定し、回線異常による切断要求の場合にはタイムに設

定する時間だけ異常チャネルを復旧用に予約しておき、相手電話番号の照合やユーザ・ユーザ情報の識別コードにより復旧対象を特定して再接続するようにしたもので、以下の方法を特徴とする。

【0011】（第1の発明）ISDN接続機器からISDN交換機を介してISDNターミナルサーバに接続メッセージを送信してチャネル接続し、切断メッセージを送信してチャネルを解放するISDN回線の接続方法において、前記ISDN接続機器は、チャネル切断時に前記切断メッセージの理由表示情報として「正常切断」を送信し、前記ターミナルサーバは、前記ISDN接続機器とのチャネル接続時にその電話番号を記録しておき、前記ターミナルサーバは、受信した前記切断メッセージに前記「正常切断」が含まれないときに回線復旧タイマの時間だけ当該チャネルを復旧待ち状態とし、このチャネルに対する前記接続メッセージの受信時に前記電話番号が一致するときにチャネル接続を許可することを特徴とする。

【0012】（第2の発明）ISDN接続機器からISDN交換機を介してISDNターミナルサーバに接続メッセージを送信してチャネル接続し、切断メッセージを送信してチャネルを解放するISDN回線の接続方法において、前記ターミナルサーバは、前記ISDN接続機器とのチャネル接続時にその電話番号を記録しておき、前記ターミナルサーバは、受信した前記切断メッセージの生成源がISDN接続機器でないときに回線復旧タイマの時間だけ当該チャネルを復旧待ち状態とし、このチャネルに対する前記接続メッセージの受信時に前記電話番号が一致するときにチャネル接続を許可することを特徴とする。

【0013】（第3の発明）ISDN接続機器からISDN交換機を介してISDNターミナルサーバに接続メッセージを送信してチャネル接続し、切断メッセージを送信してチャネルを解放するISDN回線の接続方法において、前記ISDN接続機器は、チャネル切断時に前記切断メッセージにユーザ・ユーザ情報要素を付加して伝送し、前記ターミナルサーバは、前記ISDN接続機器とのチャネル接続時にその電話番号を記録しておき、前記ターミナルサーバは、受信した前記切断メッセージに前記ユーザ・ユーザ情報が含まれないときに回線復旧タイマの時間だけ当該チャネルを復旧待ち状態とし、このチャネルに対する前記接続メッセージの受信時に前記電話番号が一致するときにチャネル接続を許可することを特徴とする。

【0014】（第4の発明）前記までの発明において、前記ISDN接続機器は、ユーザ・ユーザ情報として通常接続要求と回線復旧要求の識別コードを付加して伝送し、前記ターミナルサーバは、当該チャネルの復旧待ち状態で前記ユーザ・ユーザ情報が回線復旧要求の場合にチャネル接続を許可することを特徴とする。

【0015】

【発明の実施の形態】（第1の実施形態）図1は、本実施形態を示すTSのフローチャートであり、各処理手順を以下に詳細に説明する。

【0016】（S1）TSは、交換機2から切断メッセージ（DISK）を受信したときにその理由表示情報要素からPCによる「正常切断」要求か否かを判定する。

【0017】切断メッセージは、図2にフォーマット例を示すように、プロトコル識別子等の他に、メッセージ種別、理由表示情報要素、ユーザ・ユーザ情報要素を伝送できる。メッセージ種別には、チャネル切断（DISK）のメッセージ種別を記述できる。理由表示情報要素には、図3にフォーマットを示すように、切断理由表示値を記述できる。ユーザ・ユーザ情報要素には、図4にフォーマットを示すように、識別子に接続要求や復旧要求及び切断要求を記述できる。

【0018】この切断メッセージの通信において、PCは、正常な切断を行う場合、送信する切断メッセージの理由表示情報要素で通知する切断理由を必ず「正常切断」とする。

【0019】これにより、TSでは、切断メッセージの受信において、理由表示情報要素の理由表示値から、PCからの「正常切断」要求か、回線切断などの他の理由によるかを判定でき、PCからの切断メッセージであれば現在接続中の当該チャネルを解放する。

【0020】（S2）切断理由表示値がPCからの「正常切断」でないとき、TSは、回線異常による切断と見なし、回線復旧タイマTrを起動し、該当するチャネルを復旧待ち状態とする。

【0021】（S3）TSは、タイマの動作中に、復旧待ち状態のチャネルに対してPCから接続メッセージ（SETUP）を受信したか否かをチェックする。

【0022】接続メッセージは、図5にフォーマット例を示すように、メッセージ種別、伝達能力情報要素、チャネル識別子情報要素、発番号情報要素、ユーザ・ユーザ情報要素等を伝送できる。メッセージ種別には、チャネル接続（SETUP）のメッセージ種別を記述できる。

【0023】（S4）TSは、接続メッセージを受信したとき、回線切断前にチャネル接続していたPCであるか否かをその電話番号が一致するか否かでチェックする。

【0024】TSは、チャネル毎に相手PCの電話番号を記録するためのテーブルを持ち、チャネル接続時に、接続メッセージに含まれる発番号情報要素の内容から相手PCの電話番号を記録しておき、この記録しておいた電話番号と今回の接続メッセージに含まれる電話番号との比較でその一致／不一致をチェックする。

【0025】（S5）このチェックで電話番号が一致する場合、TSは回線接続を許可し、タイマTrを停止す

る。

【0026】(S6) TSは、相手PCの電話番号が記録されている電話番号と異なる場合、接続(着信)を拒否する。

【0027】(S7) TSは、処理S3における接続メッセージの受信がないとき、又は処理S6における電話番号不一致で着信拒否した場合、タイマTrがタイムアウトしたか否かをチェックする。

【0028】(S8) TSは、タイマTrがタイムアウトしたとき、回線の復旧が不可能であるとして、該当するチャネルを解放状態とし、他のPCからの接続も受付可能とする。

【0029】したがって、本実施形態によれば、回線切断理由により回線の一時的障害による回線異常を判定した復旧方法になり、回線異常などPCからの「正常切断」以外の回線切断には、タイマにより一定時間だけそれまで接続していたPCからの接続メッセージを待ち、当該PCからの接続メッセージの受信で回線を再接続するという回線復旧を自動的に行うことができる。

【0030】(第2の実施形態)図6は、本実施形態を示すTSのフローチャートである。同図が図1と異なる部分は、処理S11にある。

【0031】(S11) TSは、交換機から受信した切断メッセージに含まれる切断の生成源が、「ユーザ」か否(交換機である)かをチェックする。

【0032】このチェックで、切断の生成源がユーザの場合にはチャネルを解放し(S8)、ユーザでない場合には図1の場合と同様に、タイマにより一定時間だけそれまで接続していたPCからの接続メッセージを待ち、当該PCからの接続メッセージの受信で回線を再接続するという回線復旧を自動的に行う。

【0033】本実施形態は、回線切断を要求する生成源がユーザか否かにより回線異常を判定した復旧方法になる。

【0034】(第3の実施形態)図7は、本実施形態を示すTSのフローチャートである。同図が図1と異なる部分は、処理S12にある。

【0035】(S12) TSは、交換機から受信した切断メッセージにユーザ・ユーザ情報が含まれるか否かをチェックする。

【0036】PCは、正常な切断を行う場合、送信する切断メッセージへ必ずユーザ・ユーザ情報要素を付加し、このときのユーザ情報は、「切断要求」を示すユーザ特有の識別コードとする。

【0037】TSは、交換機から受信した切断メッセージにユーザ情報要素が含まれている場合にはチャネルを解放し(S8)、ユーザでない場合には図1の場合と同様に、タイマにより一定時間だけそれまで接続していたPCからの接続メッセージを待ち、当該PCからの接続メッセージの受信で回線を再接続するという回線復旧を

自動的に行う。

【0038】本実施形態は、切断メッセージにユーザ情報が含まれているか否かにより回線異常を判定した復旧方法になる。

【0039】(第4の実施形態)図8は、本実施形態を示すTSのフローチャートである。同図が図1と異なる部分は、処理S13及び処理S14にある。

【0040】(S13) TSは、交換機から受信した切断メッセージに含まれる理由表示値が「正常切断」否かをチェックする。

【0041】PCは、送信する接続メッセージへ必ずユーザ情報要素を付加する。ユーザ情報は、ユーザ特有の識別コードとし、通常の接続の場合は「回線接続要求」、回線復旧のための接続の場合は「回線復旧要求」とする。また、PCは、正常な切断を行う場合、送信する切断メッセージの理由表示情報要素で通知される切断理由を必ず「正常切断」とする。

【0042】TSは、交換機から受信した切断メッセージに含まれる理由表示値が「正常切断」の場合にはチャネルを解放し(S8)、理由表示値が「正常切断」でない場合には、タイマにより一定時間だけそれまで接続していたPCからの接続メッセージを待つ(S2, S3)。

【0043】(S14) TSは、復旧待ち状態のチャネルに対する接続メッセージを受信した場合、含まれるユーザ情報が「回線接続要求」の場合は着信を拒否し(S6)、「回線復旧要求」の場合は接続を許可してタイマTrを停止する(S5)。

【0044】本実施形態は、切断メッセージの理由表示値が「正常切断」か否かを判定し、正常切断でない場合の接続メッセージに含まれるユーザ情報が回線復旧要求か否かにより復旧接続を判定した復旧方法になる。

【0045】(第5の実施形態)図9は、本実施形態を示すTSのフローチャートである。同図が図8と異なる部分は、処理S13に代えて図6の処理S11とした点にある。

【0046】(S11) TSは、交換機から受信した切断メッセージに含まれる切断の生成源が、「ユーザ」か否(交換機である)かをチェックする。

【0047】このチェックで、切断の生成源がユーザの場合にはチャネルを解放する(S8)。

【0048】また、ユーザでない場合には、タイマにより一定時間だけそれまで接続していたPCからの接続メッセージを待ち(S2)、復旧待ち状態のチャネルに対する接続メッセージを受信した場合(S3)、含まれるユーザ情報が「接続要求」か「復旧要求」を判定し(S14)、「接続要求」の場合は着信を拒否し(S6)、「復旧要求」の場合は接続を許可してタイマTrを停止する(S5)。

【0049】本実施形態は、回線切断を要求する生成源

がユーザが否かにより正常切断が否かを判定し、接続メッセージに含まれるユーザ情報が回線復旧要求が否かにより復旧接続を判定した復旧方法になる。

【0050】（第6の実施形態）図10は、本実施形態を示すTSのフローチャートである。同図が図8と異なる部分は、処理S13に代えて図7の処理S12とした点にある。

【0051】（S12）TSは、交換機から受信した切断メッセージにユーザ・ユーザ情報が含まれるが否かをチェックする。

【0052】このチェックにおいて、ユーザ情報が含まれている場合にはチャンネルを解放し（S8）、ユーザ情報が含まれていない場合にはタイムにより一定時間だけそれまで接続していたPCからの接続メッセージを待ち（S2）、復旧待ち状態のチャンネルに対する接続メッセージを受信した場合（S3）、含まれるユーザ情報が「接続要求」か「復旧要求」を判定し（S14）、「接続要求」の場合は着信を拒否し（S6）、「復旧要求」の場合は接続を許可してタイムT_rを停止する（S5）。

【0053】本実施形態は、切断メッセージにユーザ情報が含まれているか否かにより「正常切断」が否かを判定し、正常切断でない場合に接続メッセージに含まれるユーザ情報が復旧要求が否かにより復旧要求を判定した復旧方法になる。

【0054】

【発明の効果】以上のとおり、本発明によれば、切断メッセージに含まれる切断理由や切断要求の生成源又はユーザ・ユーザ情報の有無により正規の切断要求か回線異常による切断要求かを判定し、回線異常による切断要求の場合にはタイムに設定する時間だけ異常チャンネルを復旧用に予約しておき、相手電話番号の照合やユーザ・ユーザ情報の識別コードにより復旧対象を特定して再接続

するようにしたため、以下の効果がある。

【0055】（1）回線異常の復旧を自動的に行うことにより、ユーザが回線異常を意識することなく操作を行うことができる。

【0056】（2）回線異常のチャンネルを一定期間予約しておくことにより、確実な復旧を行うことができる。

【0057】（3）特別な呼制御シーケンスを用いることなく、通常の呼制御シーケンスの中で実現することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態を示すフローチャート。

【図2】切断メッセージのフォーマット例。

【図3】理由表示情報要素のフォーマット。

【図4】ユーザ・ユーザ情報要素のフォーマット。

【図5】接続メッセージのフォーマット例。

【図6】本発明の第2の実施形態を示すフローチャート。

【図7】本発明の第3の実施形態を示すフローチャート。

【図8】本発明の第4の実施形態を示すフローチャート。

【図9】本発明の第5の実施形態を示すフローチャート。

【図10】本発明の第6の実施形態を示すフローチャート。

【図11】ISDNを用いたPC-LAN間接続システム構成例。

【符号の説明】

1...1_N...ISDN接続機器

2...ISDN公衆網交換機

3...ISDNターミナルサーバ

【図2】

切断メッセージ(DISC)のフォーマット例

ビット	8	7	6	5	4	3	2	1	
	プロトコル識別子								オクテット1
	呼番号長								オクテット2
	呼番号								オクテット3
	メッセージ識別(DISC)								オクテット4
									オクテット5
									...
	理由表示情報要素								...
									...
	ユーザ・ユーザ情報要素(オプション)								...

【図3】

理由表示情報要素のフォーマット例

ビット	8	7	6	5	4	3	2	1	
情報要素識別子(理由表示)									オクテット1
理由表示内容長									オクテット2
コネクト標準					生成源				オクテット3
仕様種別									オクテット3
理由表示値									オクテット4
診断情報(オプション)									オクテット5

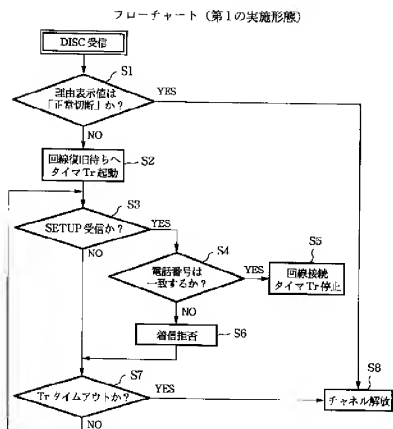
【図4】

ユーザ・ユーザ情報要素のフォーマット例

ビット	8	7	6	5	4	3	2	1	
	情報要素識別子(ユーザ・ユーザ)								オクテット1
	ユーザ・ユーザ内容長								オクテット2
	プロトコル識別子								オクテット4
	ユーザ情報								オクテット5
									...
									...

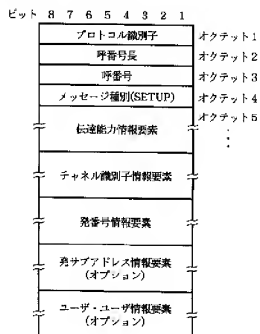
ユーザ固有識別子<例>
 10H: 接続要求
 20H: 復旧要求
 30H: 切断要求

【図 1】



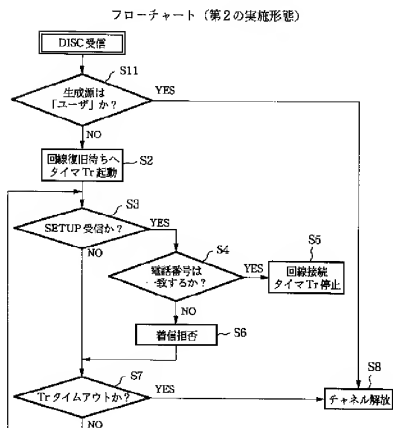
【図 5】

接続メッセージ(SETUP)のフォーマット例

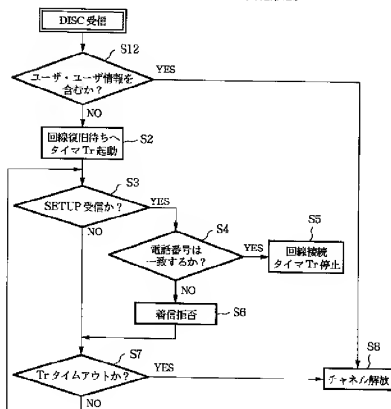


【図 7】

【図 6】

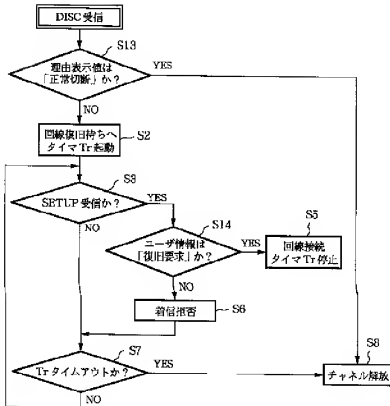


フローチャート（第3の実施形態）



【図 8】

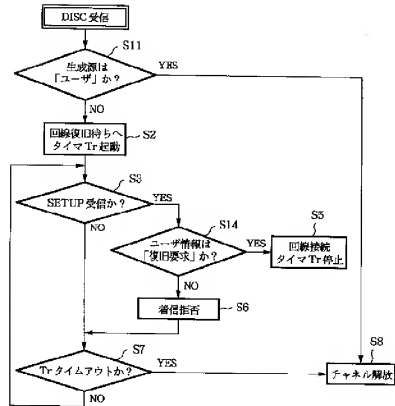
フローチャート（第4の実施形態）



【図 10】

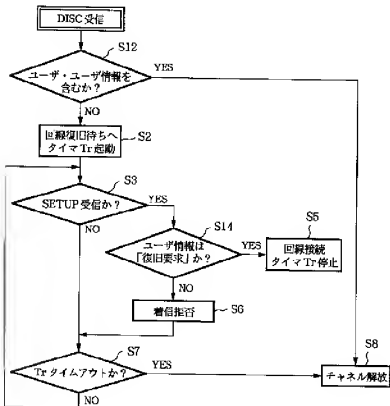
【図 9】

フローチャート（第5の実施形態）

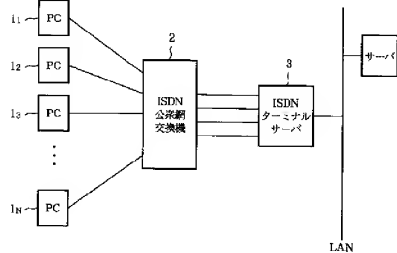


【図 11】

フローチャート（第6の実施形態）



ISDNを用いたPC-LAN間接続システム構成例



JP2000078555A CHARGING METHOD AND DEVICE FOR DATA TRANSMISSION SYSTEM

Bibliography

DWPI Title

Accounting procedure for data transmission system, manages billing of data provision depending of delivery form of encryption key whenever communication channel is established

Original Title

CHARGING METHOD AND DEVICE FOR DATA TRANSMISSION SYSTEM

Assignee/Applicant

Standardized: **SONY CORP**

Original: SONY CORP

Inventor

KUBOTA ICHIRO

Publication Date (Kind Code)

2000-03-14 (A)

Application Number / Date

JP1998243906A / 1998-08-28

Priority Number / Date / Country

JP1998243906A / 1998-08-28 / JP

Abstract

PROBLEM TO BE SOLVED: To realize charging for a data unit or a data class and for each contractor while keeping confidentiality of the data in the case of using a high speed data channel with a large capacity such as a digital CATV channel or a satellite broadcast to conduct a data service.

SOLUTION: The device has an encryption module that encodes data and serves encrypted data and a key management module 12 that manages an encryption key to decode the encrypted data and the distribution of the encryption key, and the device transmits the encrypted data to a receiver side terminal 2 via a satellite circuit 3 and transmits the encryption key to the receiver side terminal 2 via the Internet 4. A customer management module 14 manages charging of data received by the receiver side terminal 2 depending on a distribution form of the encrypted key transmitted from the key management module 12 to the receiver side terminal 2.

(51)Int.Cl. ⁷	識別記号	F I	テラコト* (参考)
H 0 4 N 7/16		H 0 4 N 7/16	C
H 0 4 H 1/02		H 0 4 H 1/02	E
H 0 4 L 12/14		H 0 4 L 11/02	F

審査請求 未請求 請求項の数18 ○L (全 18 頁)

(21)出願番号 特願平10-243906

(22)出願日 平成10年8月28日 (1998.8.28)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川 6丁目7番35号

(72)発明者 窪田 一郎

東京都品川区北品川 6丁目7番35号 ソニー株式会社内

(74)代理人 100067736

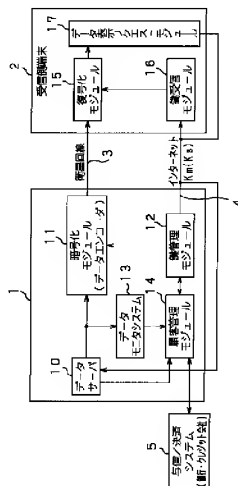
弁理士 小池 晃 (外2名)

(54)【発明の名称】 データ伝送システムの課金方法及び装置

(57)【要約】

【課題】 衛星放送やデジタルCATV回線のような大容量で高速なデータ回線を使用してデータサービスを行う場合に、データの秘密性を維持しつつデータ単位やデータ種別毎の課金、更には契約者毎の課金を実現する。

【解決手段】 データを暗号化して提供する暗号化モジュール11と、暗号化されたデータの当該暗号化を解くための暗号鍵の管理及びその暗号鍵の配信を管理する鍵管理モジュール12とを有し、暗号化したデータは衛星回線3を介して受信側端末2に送信し、暗号鍵はインターネット4を介して受信側端末2に送信する。受信側端末2にて受信したデータに対する課金は、顧客管理モジュール14が、鍵管理モジュール12から受信側端末2に送信された暗号鍵の配信形態に応じて管理する。



【特許請求の範囲】

【請求項 1】 通信回線を利用してデータを提供し、このデータ提供に対応した課金を行うデータ伝送システムの課金方法において、

上記データを暗号化して提供し、

上記暗号化されたデータの当該暗号化を解くための暗号鍵を管理し、

上記暗号鍵を配信し、

上記暗号鍵の配信形態に応じて上記課金を管理することを特徴とするデータ伝送システムの課金方法。

【請求項 2】 少なくとも通信路が確立される毎に上記暗号鍵を配信することを特徴とする請求項 1 記載のデータ伝送システムの課金方法。

【請求項 3】 少なくとも通信路が確立されている時間中に定期的に上記暗号鍵を配信することを特徴とする請求項 1 記載のデータ伝送システムの課金方法。

【請求項 4】 上記暗号鍵の配信回数を管理し、当該暗号鍵の配信回数に応じて課金を管理することを特徴とする請求項 2 記載のデータ伝送システムの課金方法。

【請求項 5】 上記暗号鍵の配信回数を管理し、当該暗号鍵の配信回数に応じて課金を管理することを特徴とする請求項 3 記載のデータ伝送システムの課金方法。

【請求項 6】 通信路が確立されている接続時間を計測し、当該接続時間に応じて課金を管理することを特徴とする請求項 1 記載のデータ伝送システムの課金方法。

【請求項 7】 各通信路毎のデータ伝送量を計測し、当該データ伝送量の総和に応じて課金を管理することを特徴とする請求項 1 記載のデータ伝送システムの課金方法。

【請求項 8】 伝送するデータ種別により上記暗号鍵を対応させ、当該データ種別による暗号鍵に応じて課金を管理することを特徴とする請求項 1 記載のデータ伝送システムの課金方法。

【請求項 9】 上記通信回線は高速の第 1 のデータ伝送路と、当該第 1 のデータ伝送路よりも低速の第 2 のデータ伝送路とからなり、上記第 1 のデータ伝送路にて上記暗号化されたデータを伝送し、上記第 2 のデータ伝送路にて上記暗号鍵を伝送することを特徴とする請求項 1 記載のデータ伝送システムの課金方法。

【請求項 10】 通信回線を利用してデータを提供し、このデータ提供に対応した課金を行うデータ伝送システムの課金装置において、上記データを暗号化して提供するデータ提供手段と、上記暗号化されたデータの当該暗号化を解くための暗号

鍵の管理及びその暗号鍵の配信を管理する鍵管理手段と、

上記暗号鍵の配信形態に応じて上記課金を管理する課金管理手段とを有することを特徴とするデータ伝送システムの課金装置。

【請求項 11】 上記鍵管理手段は、少なくとも通信路が確立される毎に上記暗号鍵を配信することを特徴とする請求項 10 記載のデータ伝送システムの課金装置。

【請求項 12】 上記鍵管理手段は、少なくとも通信路が確立されている時間中に定期的に上記暗号鍵を配信することを特徴とする請求項 10 記載のデータ伝送システムの課金装置。

【請求項 13】 上記鍵管理手段は、上記暗号鍵の配信回数を管理し、上記課金管理手段は、当該暗号鍵の配信回数に応じて課金を管理することを特徴とする請求項 11 記載のデータ伝送システムの課金装置。

【請求項 14】 上記鍵管理手段は、上記暗号鍵の配信回数を管理し、上記課金管理手段は、当該暗号鍵の配信回数に応じて課金を管理することを特徴とする請求項 12 記載のデータ伝送システムの課金装置。

【請求項 15】 通信路が確立されている接続時間を計測する接続時間計測手段を備え、上記課金管理手段は、当該接続時間に応じて課金を管理することを特徴とする請求項 10 記載のデータ伝送システムの課金装置。

【請求項 16】 各通信路毎のデータ伝送量を計測するデータ伝送量計測手段を備え、上記課金管理手段は、当該データ伝送量の総和に応じて課金を管理することを特徴とする請求項 1 記載のデータ伝送システムの課金装置。

【請求項 17】 上記鍵管理手段は、伝送するデータ種別により上記暗号鍵を対応させ、上記課金管理手段は、当該データ種別による暗号鍵に応じて課金を管理することを特徴とする請求項 10 記載のデータ伝送システムの課金装置。

【請求項 18】 上記通信回線は高速の第 1 のデータ伝送路と、当該第 1 のデータ伝送路よりも低速の第 2 のデータ伝送路とからなり、上記データ提供手段は、上記暗号化されたデータを上記第 1 のデータ伝送路に伝送し、上記鍵管理手段は、上記暗号鍵を上記第 2 のデータ伝送路に伝送することを特徴とする請求項 10 記載のデータ伝送システムの課金装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信回線を利用してデータを提供し、このデータ提供に対応した課金を行うデータ伝送システムの課金方法及び装置に関する。

【0002】

【従来の技術】衛星放送やデジタルケーブルテレビジョン（以下、CATVと記す）回線のような大容量のデータ回線を使用してデータサービスを行う場合には、先行しているデジタルオーディオ／ビデオサービスで用いられているトランスポートストリーム（Transport Stream、以下TSと記す）パケットにインターネットプロトコル（Internet Protocol、以下IPと記す）等のデータパケットを重量させ、データサービスを行う事が一般的である。

【0003】従って、データサービスの顧客管理を行う上で一番簡単な方法としては、TS毎のスクランブルを行うICカードによる限定アクセス機能（Conditional Access、以下適宜CAと記す）を用いる方法が挙げられる。この場合、TS毎のスクランブルには、TSパケットのPaket ID（Packet Identification、以下PIDと記す）によって識別される特定の暗号化キーを用いた、マルチプレクサによるスクランブル処理が行われる。

【0004】例えばインターネットサービスシステムの場合は、送出側において、ある帯域を占有する一つのエンコーダが、サービス（チャンネル）として定義される特定のPIDを持つTSパケットを生成し、このTSパケットの中に、複数ユーザのパersoナルコンピュータ（PC）へのIPデータグラムが多重される。

【0005】ICカードによるCA機器を用いた場合、ユーザグループ（例えば一つの企業）と他のユーザグループの間では、それぞれエンコーダが異なり、違ったスクランブル鍵を持つため、当該スクランブル鍵が破れない限り、互いに相手のデータを盗み見る事は不可能である。

【0006】一方、グループ内では、既にスクランブルが解かれたデータを受信可能であるため、不正に他人のデータを盗み見る事が可能である。但し、ユーザグループが一企業であり、専用線的な使い方をする場合、特にデータの不正読み出しについて注意を払う必要が無い。

【0007】

【発明が解決しようとする課題】しかしながら、一つのサービス（チャンネル）を利用して不特定多数のユーザに対してデータサービスを提供するような時には、この点が問題となる。すなわち、一般のホームページのような、誰でもアクセス可能なデータについては他人に見られても問題は無いと思われるが、いわゆるSOHO（Small Office HomeOffice）のユーザのように、仕事上秘密性の高いデータのやりとりを行う場合には、データを他人に見られる事は非常に問題となり、したがってデータの秘密性を保つ為の手段が必要となる。

【0008】また、衛星放送やデジタルCATV回線等を使用したデータサービスを行う場合、ユーザに提供

したデータに対する課金のシステムを構築しなければならない。衛星デジタル放送では、ICカードによる課金システムが既に構築されているが、このICカードによる課金システムは、元々オーディオ及びビデオ放送の番組単位の課金を基本としたシステムであり、データ単位やデータ種別毎の課金には必ずしも適していない。

【0009】そこで、本発明はこのような状況に鑑みてなされたものであり、衛星放送やデジタルCATV回線のような大容量で高速なデータ回線を使用してデータサービスを行う場合において、データの秘密性を維持しつつデータ単位やデータ種別毎の課金、更には契約者毎の課金を実現する、データ伝送システムの課金方法及び装置を提供することを目的とする。

【0010】

【課題を解決するための手段】本発明のデータ伝送システムの課金方法及び装置は、通信回線を利用してデータを提供し、このデータ提供に対応した課金を行うデータ伝送システムの課金方法であり、データを暗号化して提供し、その暗号化されたデータの当該暗号化を解くための暗号鍵を管理してその暗号鍵を配信すると共に、そのときの暗号鍵の配信形態に応じて課金を管理することにより、上述した課題を解決する。

【0011】

【発明の実施の形態】本発明の好ましい実施の形態について、図面を参照しながら説明する。

【0012】以下、本発明にかかるデータ伝送システムの課金方法及び装置が適用される一実施の形態であるデータサービスシステムの全体構成について、図1を用いて説明する。

【0013】図1に示すデータサービスシステムにおいて、データ送信装置1のデータサーバ10は、例えばオーディオデータやビデオデータ等だけでなく、コンピュータプログラム等の各種データをデジタルコンテンツとして格納してなるものである。本実施の形態では、特にデータサービスを例に挙げているため、当該データサーバ10から取り出されるデジタルコンテンツをコンピュータプログラム等の各種データ（以下、単にデータとする）として説明する。このデータサーバ10から出力されたデータは、暗号化モジュール11に送られる。

【0014】暗号化モジュール（データエンコーダ）11は、鍵管理モジュール12から送られてきた暗号鍵を用いて、上記データサーバ10からのデータを暗号化し、当該暗号化データを、例えば衛星回線やデジタルCATV回線等の大容量且つ高速の通信回線に送信（配信）する。

【0015】ここで、本実施の形態では、通信回線として衛星デジタル放送に使用される衛星回線3を用いた場合を例に挙げている。したがって当該暗号化モジュール11では、上記データサーバ10からのデータをIP（Internet Protocol）等のデータパケットにパケット

化（すなわち I P データグラムを生成）して暗号化し、この暗号化データ（以下、セクションデータとする）に所定の付加情報（例えば MAC（Media Access Control）アドレスを含むヘッダ等）を付加したデータを、デジタルオーディオ／ビデオサービスで用いられているような TS（Transport Stream）パケットに重畳させ、当該 TS パケットを衛星回線 3 に送信（すなわち配信）するようにしている。なお、このデータサーバ 10 における I P データグラムの生成及び暗号化モジュール 11 における暗号化処理（セクションデータの生成処理）の詳細及び具体的構成、当該セクションデータ及びそのヘッダに含まれる MAC アドレス等の詳細については後述する。

【0016】鍵管理モジュール 12 は、上記暗号化モジュール 11 における I P データグラムの暗号化に使用する暗号鍵を管理する。この鍵管理モジュール 12 からの暗号鍵は、電話回線及び ISDN（Integrated Services Digital Network：統合サービスデジタル通信網）等を使用した地上回線を介して伝送される。本実施の形態では、当該地上回線として、電話回線又は ISDN 等を使用したインターネット 4 を例に挙げている。上記鍵管理モジュール 12 がインターネット 4 を介して受信側端末 17 に送信する暗号鍵は、セキュリティ確保のため当然暗号化されているものとする。当該鍵管理モジュール 12 が管理する暗号鍵、及びこの暗号鍵の送信並びに暗号化等の詳細については後述する。

【0017】受信側端末 17 の鍵受信モジュール 16 は、上記インターネット 4 を介して送信されてきた上記暗号鍵を受信して復号（暗号解読）し、当該受信及び復号した暗号鍵を受信側端末 17 内の復号化モジュール 15 に転送する。

【0018】復号化モジュール 15 は、上記衛星回線 3 を介して受信したデータの TS パケットから前記セクションデータを取り出し、当該セクションデータのヘッダに含まれる MAC（Media Access Control）アドレスに基づいて、対応する暗号鍵を鍵受信モジュール 16 から受け取り、当該暗号鍵を用いて上記セクションデータ内の暗号化された I P データグラムの暗号解読（データデコード）を行う。なお、当該復号化モジュール 15 における暗号解読の詳細については後述する。

【0019】データ表示リクエストモジュール 17 は、提供を受けたいデータのリンク先を、例えばインターネット 4 を通じてデータ送信装置 1 に送信し、また、必要に応じて表示を行う。

【0020】データ送信装置 1 のデータモニタシステム 13 は、個々の契約者の受信側端末 2 に対して送信（配信）されるデータ量（情報量）や通信路が確立された接続時間などをモニタする。例えば送信されるデータ量をモニタする場合には、送信されるデータのアドレス毎のデータ量或いはパケット毎のデータ量を集計し、また、

接続時間をモニタする場合には、図示しない内部時計からの時間情報に基づいて当該接続時間を集計する。

【0021】また、データ送信装置 1 の顧客管理モジュール 14 は、上記鍵管理モジュール 12 に対して指令を行い、当該鍵管理モジュール 12 による暗号鍵の配信をどのように行うかを管理する。また、顧客管理モジュール 14 は、契約者毎の契約形態やデータ単位毎或いはデータ種別毎の課金形態によって様々な課金方法の管理を行うと共に、それら契約形態や課金方法に基づいて契約者毎の課金情報の集計及び管理を行う。さらに、顧客管理モジュール 14 は、金融／クレジット会社等の与信／決済システム 5 と回線が繋がっており、したがって、当該顧客管理モジュール 14 は、当該与信／決済システム 17 を通じて、上記集計された課金情報に基づいた個々の契約者への請求書の発行及び入金管理等を行う。

【0022】ここで、本実施の形態のようなデータサービスシステムにおける契約者の契約形態としては、以下の 3 種類の契約形態（第 1 ～ 第 3 の契約形態）が考えられる。

【0023】「第 1 の契約形態」データサービスを受ける事が可能な契約を一旦行えば、受信するデータ種別／データ量にかかわらず、一定の課金となされる契約形態（フラット／定額制課金）。

【0024】「第 2 の契約形態」受信するデータ量によって課金される契約形態（従量制課金）。

【0025】「第 3 の契約形態」受信するデータ種別によって課金される契約形態（コンテンツ課金）。

【0026】このため、上記顧客管理モジュール 14 は、データサービスにおいて契約者によりなされる課金設定により、上記第 1 ～ 第 3 までの契約形態のうち何れか一つを選択する。

【0027】先ず、上記第 1 の契約形態（フラット／定額制課金）にて契約がなされた場合、契約者（受信側端末 2）は、暗号鍵を一旦受け取った後はそのまま当該暗号鍵を更新する事無く、ずっと使える事になり、最も簡単且つ便利である。

【0028】この第 1 の契約形態にて契約がなされた場合の課金は、例えば毎月一定額の課金等が考えられ、したがって、上記顧客管理モジュール 14 では、当該第 1 の契約形態を選択した契約者に対しては当該毎月一定額となるような課金を、上記与信／決済システム 17 を通じて行う。なお、当該第 1 の契約形態にて契約がなされた場合における課金のための具体的構成及び動作の詳細については後述する。

【0029】ただし、暗号鍵を変更せずに常に同一の暗号鍵を使用していると、例えばハッカー等によって暗号鍵が解明される恐れがある為、一般にはあるタイミングで暗号鍵を変更する必要がある。

【0030】上記暗号鍵を変更するタイミングとしては、以下の 3 種類の変更タイミング（第 1 ～ 第 3 の暗号

鍵変更タイミング)が考えられる。

【0031】「第1の暗号鍵変更タイミング」暗号鍵の不正解読等の問題が発生するまで暗号鍵の変更を行わない。言い換えれば、問題が発生したタイミングで暗号鍵を変更する。

【0032】「第2の暗号鍵変更タイミング」通信路(セッション)が確立される毎に暗号鍵を配信する。すなわち、通信路が確立される毎のタイミングで異なる暗号鍵を配信する。

【0033】「第3の暗号鍵変更タイミング」通信路(セッション)が確立されて通信を行っている時間中は定期的に暗号鍵の配信を行う。すなわち、通信路が確立されて通信を行っている時間中の定期的なタイミングで異なる暗号鍵を配信する。

【0034】これら3つの暗号鍵変更タイミングは第1の暗号鍵変更タイミングから順にセキュリティ性が高くなっており、システムへのセキュリティへの要求度によってどの変更タイミングを取るかを決定すれば良い。

【0035】次に、上記第2の契約形態(従量制課金)にて契約がなされた場合、すなわち、受信するデータ量によって課金を行う場合は、契約者(受信側端末2)が受信したデータ量(言い換えればデータ送信装置1が送信したデータ量)を計測しなければならない。このデータ量の計測方法としては、以下の3種類の計測方法(第1～第3のデータ量計測方法)が考えられる。

【0036】「第1のデータ量計測方法」通信路(セッション)が確立されて通信を行っている時間中は定期的に暗号鍵の配信を行う上記第3の暗号鍵変更タイミングの場合において、通信路(セッション)が確立されている期間中に配信される暗号鍵の配信回数を数え、この配信回数からデータ量を計測する。

【0037】「第2のデータ量計測方法」通信路(セッション)が確立されている期間の接続時間を計り、この接続時間からデータ量を計測する。

【0038】「第3のデータ量計測方法」各通信路(セッション)毎の実際のデータ伝送量を計測する。例えば送信されるアドレス毎或いはパケット数からデータ量を計測する。

【0039】したがって、この第2の契約形態(従量制課金)にて契約がなされた場合の課金は、上記第1～第3のデータ量計測方法の何れを選択したかにより異なる。すなわち、第2の契約形態(従量制課金)にて契約がなされた場合の課金方法としては、上記第1～第3のデータ量計測方法に対応した以下の3種類の課金方法(第1～第3の課金方法)が考えられる。なお、当該第2の契約形態にて契約がなされた場合における課金のための具体的構成及び動作の詳細については後述する。

【0040】「第1の課金方法」上記第1のデータ量計測方法のように、通信路(セッション)の確立された期間中に配信された暗号鍵の配信回数からデータ量を計測

した場合は、当該暗号鍵の配信回数に応じて契約者への課金を行う。すなわち、この第1の課金方法の場合の上記顧客管理モジュール14では、通信路(セッション)の確立された期間中に鍵管理モジュール12が受信側端末2に配信した暗号鍵の配信回数を管理し、この配信回数に応じた課金を、上記与信/決済システム17を通して行う。

【0041】「第2の課金方法」上記第2のデータ量計測方法のように、通信路(セッション)の確立された期間中の接続時間を計ってデータ量を計測した場合は、当該接続時間に応じて契約者への課金を行う。すなわち、この第2の課金方法の場合の上記顧客管理モジュール14では、通信路(セッション)の確立された期間中にデータモニタシステム13が集計した接続時間を管理し、この接続時間に応じた課金を、上記与信/決済システム17を通して行う。

【0042】「第3の計測課金方法」上記第3のデータ量計測方法のように、各通信路(セッション)毎のデータ伝送量を直接計測した場合は、当該データ伝送量の総和に応じて契約者への課金を行う。すなわち、この第3の課金方法の場合の上記顧客管理モジュール14では、通信路(セッション)の確立された期間中にデータモニタシステム13が集計したデータ伝送量を管理し、このデータ伝送量の総和に応じた課金を、上記与信/決済システム17を通して行う。

【0043】次に、上記第3の契約形態(コンテンツ課金)にて契約がなされた場合は、受信するデータ種別(コンテンツ)によって課金を行う。すなわち、契約者(受信側端末2)に送信されるコンテンツはそれぞれコンテンツ毎に異なった暗号鍵により暗号化されているため、そのコンテンツを暗号化したときの暗号鍵は予めリクエストのあった契約者(受信側端末2)にのみ配信され、当該暗号鍵を受け取った契約者(受信側端末2)だけが上記暗号化されたコンテンツを正しく復号し、データを取り出すことができるようになっている。このため、当該第3の契約形態のように、受信するデータ種別(コンテンツ)によって課金を行う場合は、契約者(受信側端末2)に受信した暗号鍵(暗号化されたコンテンツの暗号解読を行うための暗号鍵)に応じた課金、言い換えれば契約者(受信側端末2)に対して送信した暗号鍵に応じた課金を行う。なお、この第3の契約形態の場合、課金される金額は、データ種別すなわちコンテンツに応じて異なる額としたり、データの重要度に応じて異なる額とすることも可能である。言い換えれば、契約者(受信側端末2)に送った暗号鍵の種類によって、課金の額を変更することが可能である。

【0044】したがって、この第3の契約形態の場合の上記顧客管理モジュール14では、鍵管理モジュール12が契約者(受信側端末2)に対して送信した暗号鍵に応じた課金を、上記与信/決済システム17を通して行

う。なお、当該第3の契約形態にて契約がなされた場合における課金のための具体的構成及び動作の詳細については後述する。

【0045】次に、上述したような第1～第2の契約形態にて契約がなされた場合において、課金のための図1の顧客管理モジュール14の具体的構成及び動作について、図2を参照しながら説明する。

【0046】この図2において、顧客管理モジュール14は、個々の契約者毎の契約形態（前記第1～第3の契約形態）及び前記第1～第3の暗号鍵変更タイミング、第1～第3のデータ量計測方法、第1～第3の課金方法についての各情報を顧客情報として格納する顧客データベース21を有すると共に、個々のデータ種別毎のコンテンツリストを格納して個々のデータ種別毎にその情報量を管理するコンテンツ管理サーバ20を有している。

【0047】先ず最初に、前記第1の契約形態（フラット／定額制課金）の場合の顧客管理モジュール14における課金処理の流れについて説明する。

【0048】契約者（受信側端末2）から通信路（セッション）確立の要求（リクエスト）がインターネット4等の地上回線を経由してなされた場合、このリクエストは一旦、鍵管理モジュール12に転送される。当該リクエストを受け取った鍵管理モジュール12は、顧客管理モジュール14の顧客認証／鍵管理モジュール制御部23に対して、暗号鍵の配信要求を行う。

【0049】顧客認証／鍵管理モジュール制御部23は、顧客データベース21に格納した顧客情報を用いて、このリクエストを行った契約者の契約情報をチェックし、暗号鍵を与えて良いか否かを判断し、与えて良いと判断された場合は、その顧客情報に記述された鍵配信の形態と合わせて、暗号鍵の配信を鍵管理モジュール12に指示する。また同時に、顧客認証／鍵管理モジュール制御部23は、利用履歴ログ収集部24に対して当該リクエストを行った契約者（受信側端末2）の利用履歴を登録し、利用料課金処理部25に対して例えば毎月のある期日にその利用状況に応じた課金処理を行い、さらに請求・収納・支払・滞納管理部26を介して銀行やクレジット会社等の与信／決済システム5に対して契約者への請求書の発行依頼等を行う。

【0050】次に、前記第2の契約形態（従量制課金）を行う場合の顧客管理モジュール14における課金処理の流れについて説明する。

【0051】当該第2の契約形態のように、伝送された情報量（前記暗号鍵の配信回数や接続時間、データ伝送量）に応じた課金を行う場合には、前述したように図1の鍵管理モジュール12における暗号鍵の配信回収や、図1のデータモニタシステム13におけるアドレス毎のデータ量（或いはパケット数）又は接続時間、データ伝送量等の集計情報の取得／集計結果が、顧客認証／鍵管理モジュール制御部23に転送される。顧客認証／鍵管

理モジュール制御部23では、この集計情報の取得／集計結果に基づいて、利用履歴ログ収集部24に対して当該データの提供を受けた契約者（受信側端末2）の利用履歴のログを取り、利用料課金処理部25に対して例えば毎月のある期日にその利用状況に応じた課金処理を行い、請求・収納・支払・滞納管理部26を介して与信／決済システム5に対して契約者への請求書の発行依頼等を行う。

【0052】次に、前記第3の契約形態（コンテンツ課金）を行う場合の顧客管理モジュール14における課金処理の流れについて説明する。

【0053】当該第3の契約形態のように、受信するデータ種別によって課金がなれる場合は、先ずデータサーバ10からコンテンツ課金を行うデータ種別の一覧（コンテンツの一覧）がコンテンツ課金設定部22経由でコンテンツ管理サーバ20に転送されコンテンツリストに載せられることにより、データ種別の登録が行われる。

【0054】コンテンツ課金設定部22では、データ種別すなわちコンテンツ種別とそのコンテンツの暗号化のための暗号鍵の設定を、鍵設定通知として鍵管理モジュール12に指示する。

【0055】ここで、一旦、コンテンツ管理サーバ20にデータ種別が登録されれば、後は第1の契約形態（フラット課金／定額制課金）の場合と同様の処理が行われる。すなわち、特定のデータ種別（特定のコンテンツ）の配信の要求（リクエスト）があった場合、顧客認証／鍵管理モジュール制御部23は、当該要求者が顧客データベース21に登録された契約者であるかを判断し、またこのリクエストを行った契約者の契約情報をチェックし、暗号鍵を与えて良いか否かを判断し、さらに、与えて良いと判断された場合には、そのリクエストされたデータ種別がコンテンツ管理サーバ20のコンテンツリストに登録されているかの確認を行い、当該リクエストのあったデータ種別がコンテンツリストに登録されていると確認した場合には、そのリクエストされたデータ種別に対応する鍵配信を鍵管理モジュール12に指示する。また同時に、顧客認証／鍵管理モジュール制御部23では、利用履歴ログ収集部24に対して配信の要求を行った契約者とそのリクエストされたデータ種別の利用履歴の登録を行い、利用料課金処理部25に対して例えば毎月のある期日にその利用状況に応じた課金処理を行い、請求・収納・支払・滞納管理部26を介して与信／決済システム5に対して契約者への請求書の発行依頼等を行う。

【0056】次に、本発明実施の形態のデータサービスシステムのより概略的な構成、前記データサーバ10でのIPデータグラムの生成及び暗号化モジュール11における暗号化処理（セクションデータの生成処理）の詳細及び具体的構成、当該セクションデータ及びそのヘッ

ダに含まれるMACアドレス等の詳細、鍵管理モジュール12が管理する暗号鍵及びこの暗号鍵の送信並びに暗号化等の詳細、復号化モジュール15における暗号解読の詳細について、以下に説明する。

【0057】本発明実施の形態のデータサービスシステムは、図3に示すように、通信経路とされる衛星回線3、専用線37、電話回線38、及び双方向の通信経路39を介して、前記データ送信装置1から前記受信側端末2であるデータ受信装置2a、2b、2cに対してデータを配信するようになされており、上記データ送信装置1でデータを暗号化し、当該暗号化したデータをデータ受信装置2a、2b、2cに通信経路を介して伝送するデータサービスシステムである。

【0058】このデータサービスシステムは、データ送信装置1からデータ受信装置2a、2b、2cへのデータの伝送に使用する第1の通信経路とされる通信衛星34を利用した通信経路と、データ送信装置1からデータ受信装置2a、2b、2cとの間を双方向通信可能にする第2の通信経路である専用線37、電話回線38、及び双方向の通信経路39とを有している。そして、データサービスシステムは、データ送信装置1からデータ受信装置2a、2b、2cへ送る暗号化したデータの伝送には、上記第1の通信経路を用い、データ送信装置1からデータ受信装置2a、2b、2cへの前記暗号鍵の伝送には、上記第2の通信経路を用いている。第2の通信経路は、前記インターネット4と接続されている。

【0059】上記データ送信装置1は、上記各通信回線を利用してデータ受信装置2a、2b、2cへの各種データの配信を行う。データ受信装置2a、2b、2cは、各通信回線から伝送されてくるデータを受信する。なお、図1には、データ受信装置2a、2b、2cを3台として示しているが、実際には数百台から数万台のデータ受信装置（受信側端末2）が存在して当該データサービスシステムを構成している。

【0060】このデータ送信装置1とデータ受信装置2a、2b、2c（なお、以下の説明では、データ受信装置2a、2b、2cについて特定するの必要がない場合には、単にデータ受信装置2という。）との間でデータの送受信を可能にする通信経路については、次のように構成されている。

【0061】上記衛星回線3は、約30Mbpsの帯域を有するKuバンドの片方向の回線を想定する。この衛星回線3により、例えば、日本全国に分布されているデータ受信装置に対して、データ送信装置1からのデータの伝送を同時期に行うことができる。

【0062】双方向の通信経路39は、データ送信装置1とデータ受信装置2との間で、衛星回線3とは別に設けた通信経路であって、データ送信装置1とデータ受信装置2との間での双方向通信を可能にするものである。本実施の形態では、双方向の通信経路39は、イン

ターネット4での通信に用いる汎用の通信経路を想定している。

【0063】専用線37は、データ送信装置1とデータ受信装置2とを直接接続している通信手段である。

【0064】上記インターネット4は、いわゆる映像情報、音楽情報等の各種情報を提供するものであって、いわゆるインターネットサービスプロバイダ35により、インターネット4とデータ受信装置2とは通信可能に接続されている。データ送信装置1は、インターネット4に接続されている。

【0065】なお、上述したようにデータ送信装置1とデータ受信装置2との間でデータの送受信を可能にする専用線37、電話回線38、及び双方向の通信経路39は、衛星回線3ほど大容量の帯域ではなく、数Kbpsから数百Kbps程度が通常の帯域とされる。

【0066】上記データサービスシステムは、所定のデータを特定のデータ受信装置においてのみ受信することが可能になされており、例えばデータ受信装置2aのみにデータを伝送するといった個別配信（ユニキャスト型データ配信）、又は例えばデータ受信装置2a、2bとからなる受信グループにのみデータを伝送するといったグループ宛の同報配信（マルチキャスト型データ配信）、又は全てのデータ受信装置2a、2b、2cと同時にデータを伝送するといった一斉配信（ブロードキャスト型配信）等の配信形態が可能とされて構成されている。

【0067】次に、このデータサービスシステムにおいて、データ送信装置1からデータ受信装置2へのデータの伝送について説明する。

【0068】データ送信装置1からデータ受信装置2へ伝送されるデータは、図4に示すように、データのカプセル化が施されている。このカプセル化は、データを伝送するデータ送信装置1において行われる処理であって、第1のカプセル化工程により、データ受信装置2への配信対象とされるデータを第1のプロトコルによりカプセル化し、第2のカプセル化工程により、上記第1のプロトコルによりカプセル化したデータを第2のプロトコルによってカプセル化する。ここで、カプセル化とは、データ自体に対して加工を施すことなく、当該データ自身を通信プロトコルにより規定された伝送フォーマットに基づいて構成されるカプセル（パケット又はフレーム等）に入れ込むことをいい、このカプセル化によりデータの伝送制御が可能になる。

【0069】上記第1のカプセル化工程では、データ受信装置2への配信対象とするデータの全体を含む実データ部に当該実データ部に関する付加情報部を付加してカプセル化するとともに、上記実データ部については暗号化して上記カプセル化を行う。以下に詳しく説明する。

【0070】IP（Internet Protocol）データグラム101は、図4の（a）に示すように、インターネット

プロトコルに則して構成されているデータである。このIPデータグラム101は、上記データ受信装置2への配信対象とされるデータを格納して構成されている。そして、IPデータグラムのヘッダ部には、例えば、インターネット上において使用される宛先を識別するための送信先アドレス (Destination Address) が付加されている。

【0071】なお、IPデータグラム101の部分は、インターネットプロトコルとして構成されることに限定されるものではなく、イーサネットプロトコルを採用して構成されてもよい。

【0072】そして、データ送信装置1は、図4の(b)から図4の(d)に示すように、データを上記第1のプロトコルによりカプセル化する。例えば、第1のプロトコルとしては、DVB (Digital Video Broadcasting) の Multiprotocol Encapsulation を採用している。

【0073】まず、データ送信装置1は、第1のプロトコルによるデータのカプセル化を、図4の(b)に示すように、IPデータグラムに対してパディングを行い (パディング部102を付加する)、データ部の長さを64ビットの整数倍にする。例えば、IPデータグラム101の末尾に0ビット〜63ビット長のパディングを行い、パディングするビットはすべて1とする。このパディングにより、所定のデータ長さにすることができ、これは、このIPデータグラム101とパディング部102とからなるセクションのデータ部を暗号化する際に、データ部の長さが64ビットの整数倍の方が都合が良いからである。本実施の形態では、当該第1のプロトコルのフォーマットによって構成されるデータ部分をセクションと呼んでいる。

【0074】次に、データ送信装置1は、パディング部102が付加されたセクションを、図4の(c)に示すように暗号化する。ここで、暗号化は、暗号鍵によって行うもので、暗号鍵は、上記データ受信装置2に対して配信の対象とされる情報について暗号化するために使用される後述するセッション鍵である。また、暗号化の方式としては、いわゆるTriple-DESのような共通鍵方式のブロック暗号化を用いる。このTriple-DES方式の暗号化は、公開鍵方式の中でも強力な暗号方式であり、ハードウェアによる実装で高速化も容易とされる。これにより、30Mbps程度の高速な暗号化にであっても、公開鍵方式の暗号化とは異なり、処理時間がかかってデータの伝送に間に合わなくなることを防止することができる。

【0075】そして、データ送信装置1は、図4の(d)に示すように、暗号化されたセクションデータ部104に、セクションヘッダ部103及びエラー検出のために使用されるテラ部105を付加する。

【0076】ここで、上記暗号化されたセクションデー

タ部104は、MAC (Media Access Control) フレーム化されて構成されている。このMACフレーム化により、データ部にMACヘッダが付加され、このMACヘッダ部を参照することにより、当該フレーム化されて格納されているデータの宛先の制御が容易とされるようになる。具体的には、MACフレームには、当該MACフレーム化されたデータの受信が許可されているデータ受信装置の宛先アドレスが格納されている。

【0077】上記セクションヘッダ部103は、宛先アドレスを格納する部分であって、48ビットの宛先アドレスが格納されるようにデータ空間が確保されている。具体的には、上記セクションヘッダ部103においてMACヘッダ部を構成して、宛先アドレスが格納されている。このセクションヘッダ部103に48ビットにより表現される宛先アドレスを格納できる空間を設けることにより、データ受信装置の限定範囲の種類が少ないことを解消することができる。すなわち、暗号鍵を識別するための多くの情報を格納することができるようになる。さらに、IPデータグラム101を伝送する際に、インターネットプロトコルの宛先アドレスから後述するパケットIDの対応付けを行わなくもよくなり、インターネットプロトコルの親和性を得ることができる。

【0078】また、上記テラ部105は、CRC (Cyclic Redundancy Checking、巡回冗長検査) によってコード化されている。CRCは、MACフレーム化されたデータを受信したデータ受信装置2が、当該MACフレームが正しく衛星回線において伝送されているかを検査するためのものである。例えば、CRCは、32ビットによってコード化されている。

【0079】以上が第1のプロトコルによる配信対象とされるデータのカプセル化であって、次に、この第1のプロトコルによってカプセル化されたデータを、第2のプロトコルによってカプセル化させる処理について説明する。

【0080】第2のプロトコルによるカプセル化は、上記第1のプロトコルによってカプセル化されたデータを、複数のパケットに分割することにより実行されるカプセル化である。

【0081】ここで、第2のプロトコルは、TS (Transport Stream) パケット化によるものである。MPEG 2 (Moving Picture Experts Group Phase 2) によって規格されているものであって、オーディオ、ビデオ信号やデータのような多種類のデータが多重化されて、大容量のデジタル回線で伝送することが可能になる。この第2のプロトコルにより、上記第1のプロトコルによってカプセル化されたデータは、図4の(e)乃至図4の(g)に示すように、カプセル化されて、複数のTSパケット106、107、108に分割される。上記TSパケット106、107、108は、TSヘッダ部HTSと、TSペーロード部Pとによって構成され、上記TS

ペイロード部Pには、分割されて上記第1のプロトコルによってカプセル化されたデータが格納される。そして、TSパケットのTSヘッダ部HTSには、図5に示すような、パケットID (PID) 部及びスクランブル制御部によって構成される。この図5は、一般的なTSパケットのフォーマットの構造を表しており、ヘッダ部のPID (Packet Identification) 部411及びスクランブル制御部412により暗号鍵が特定される。当該暗号鍵は、セッション鍵Kとワーク鍵Kmとがある。また、上記PID部411は13ビットのデータであり、上記スクランブル制御部412は2ビットのデータ、TSパケットのデータはペイロード部分413に記述される。なお、この図5の例では、PID部411及びスクランブル制御部412に宛先アドレスが書き込まれているが、本実施の形態においては、上述したように、宛先アドレスをセッションヘッダ部103に書き込むことにより、宛先アドレス情報が制限されることを防止している。

【0082】以上が第2のプロトコルによるカプセル化であり、よって、データ送信装置1は、データ受信装置2への配信対象とされるデータ (IPデータグラム) を第1のプロトコル及び第2のプロトコルによって多重にカプセル化して、通信衛星34への当該データの伝送を行っている。

【0083】このように、本実施の形態では、TSパケットとセッションの2つのレベルにおいてそれぞれ独立に処理してデータ伝送を行っているので、例えば利用するPIDを増加することなく、暗号鍵について多くの情報を確保することができ、また、アプリケーション毎に制御方法を用意しなくて済み、新しいアプリケーションへの素早い対応ができるようになり、さらに、認証ヘッダや暗号ペイロードを既存のインターネットで使うことができるようになる。

【0084】次に、データ送信装置1において行う暗号鍵によるデータの暗号化及びデータ受信装置2において行う暗号化されているデータの暗号鍵 (復号鍵) による復号化について説明する。

【0085】ここで、データ送信装置1における前記鍵管理モジュール12及び暗号化モジュール11と、データ受信装置2の前記鍵受信モジュール16及び復号化モジュール15は、具体的には図6に示すように構成されている。

【0086】この図6において、セッション鍵Ks124及び134は、上記データ送信装置1及び上記データ受信装置2がデータの暗号化/復号化に使用する鍵であり、いわゆる共通鍵方式が採用されている。上記データ送信装置1のセッション鍵Ks124は前記鍵管理モジュール12が管理し、上記データ受信装置2のセッション鍵Ks134は鍵受信モジュール16が復号化して生成する。

【0087】データ送信装置1の暗号化ユニット121は、セッション鍵Ks124を使用して、特定のデータ受信装置に対して送られる情報データを暗号化する。すなわち図1の暗号化モジュール11は、図4の(c)に示すセッションのデータ部を、当該セッション鍵Ks124を使用して上記Triple-DESにより暗号化する。また、データ受信装置2の復号化ユニット131は、配信されてきた暗号化されたデータをセッション鍵Ks134により復号化して意味のある情報として取り出す。

【0088】マスター鍵Km125及びKm135は、上記セッション鍵Ksと同様に、データ送信装置1及びデータ受信装置2が共に所持している暗号鍵であって、各データ受信装置2a、2b、2cに固有のものである。

【0089】マスター鍵Kmは、データ送信装置1とデータ受信装置2と間を通信処理するようなことはなく、すなわち、通信経路上に存在する場合はなく、これによりいかなる手段によっても他人によって知ることができない暗号鍵とされている。

【0090】このマスター鍵Kmは、セッション鍵Ksをデータ送信装置1からデータ受信装置2に送信する際に、セッション鍵Ksを暗号化/復号化するために用いられる。すなわち、データ送信装置1の鍵管理モジュール12に内蔵される暗号化ユニット122は、マスター鍵Km125を使用してセッション鍵Ks124を暗号化してデータ受信装置2に予め伝送しておく。データ受信装置2の鍵受信モジュール16に内蔵される復号化ユニット132は、受信した暗号化されているセッション鍵Ks124を、当該データ受信装置2が所持しているマスター鍵Km135によって復号化して取り出す (セッション鍵Ks134として取り出す)。

【0091】このマスター鍵Kmによる暗号鍵 (セッション鍵Ks) の暗号化及び復号化により、データ送信装置1からデータ受信装置2へ伝送する間に、上記暗号化されたセッション鍵Ksが盗聴者によって盗聴されたとしても、その復号化がなされることはない。

【0092】なお、このマスター鍵Kmによるセッション鍵Ksの暗号化/復号化についても、上記Triple-DESに基づいて行うが、公開暗号方式を採用することもできる。これは、公開暗号方式は、鍵の暗号化及び復号化がデータの暗号化/復号化とは異なり高速性を要求されないこと、安全性を確保することができるからである。

【0093】本実施の形態では、上記セッション鍵Ks124を、前述したように顧客管理モジュール14の管理の元で鍵管理モジュール12が管理し、このセッション鍵Ks124の配信状況に応じて前述したような課金が行われる。

【0094】ここまでの説明では、データ受信装置2がデータ送信装置1から受動的にセッション鍵Ks124を受け取る例を説明したが、双方向通信経路9を利用す

ることにより、データ受信装置2の側から能動的にセッション鍵Ksの要求を行うこともできる。これにより、各データ受信装置2a, 2b, 2cは、素早く確実に必要なセッション鍵Ks124をデータ送信装置1から取得することができる。具体的には、例えば、新たにデータ受信装置2がこのデータサービスシステムに加わる場合や、障害によりこの系から外れていたデータ受信装置2が障害から復旧して再びこのデータサービスシステムに加わる場合、またデータ受信装置2においてセッション鍵Ksが正しく受信出来なかった場合などには、データ受信装置2の側から能動的にセッション鍵Ksの要求を行うことにより、各データ受信装置2a, 2b, 2cは素早く確実に必要なセッション鍵Ksを取得することができる。例えば、上述したような障害復旧やセッション鍵Ksの更新の管理は、データ送信装置1の鍵管理モジュール12や、データ受信装置(受信側端末)2内にある鍵受信モジュール16及びデータ表示リクエストモジュール17等が、双方向に通信を行うことにより実現する。このようなことから、本実施の形態においては、例えば衛星回線のみをデータサービスシステムに組み込むことによる弊害、例えば、情報が各データ受信装置に正しく伝わったかどうかをデータ送信装置が知ることができない等といった問題を解決することができる。

【0095】なお、データ送信装置1からデータ受信装置2へのセッション鍵Ksの伝送については、片方向通信経路とされる衛星回線3を用いて行ってもよく、双方向の通信経路39によって行ってもよい。

【0096】ここで、上記セッション鍵Ksは、前記第3の暗号鍵変更タイミングのように、定期的に更新して配信される場合がある。このセッション鍵Ksの更新は、図7に示すフローチャートのような更新手順に従って実行される。

【0097】まず、ある時点において、データ受信装置2の鍵受信モジュール16は、セッション鍵Ks134として、セッション鍵Ks_evenと、セッション鍵Ks_oddの2つを保持している。データ受信装置2は、このようにセッション鍵Ksを2つ所持することにより、このセッション鍵Ks_even又はセッション鍵Ks_oddの何れかを使用して、データ送信装置1から送信されてくる情報データの復号化を行う。

【0098】ここで、現在使っているセッション鍵Ksがどちらであるかは、前記図4に示すセッションヘッダ部103に情報として書き込まれている。例えば、セッションヘッダ部103は、図8に示すように、テーブルID (table_id)、MACアドレス部 (MAC_address_1, MAC_address_2, MAC_address_3, MAC_address_4, MAC_address_5, MAC_address_6) と、セッション情報部 (section_length, section_number, last_section_number)、s s i (section_syntax_indicator)、p i (private_indicator)、r s v d (reserved)、p s c (payload_scr

amble_indicator) 111、a s c (address_scramble_indicator)、L S f (LLC_SNAP_flag)、及びc n i (current_next_indicator)によって構成されている。ここで、p s c 111が現在使っているセッション鍵Ksがどちらであるかの情報を示す。例えば、上記p s c 111は、2ビットの情報であり、例えば、p s cの上位ビットが「0」のときは、セッション鍵Ks_evenが使用されていることを示し、p s cの上位ビットが「1」のときには、セッション鍵Ks_oddが使用されていることを示す。

【0099】上述したような使用されているセッション鍵Ksの判断をステップS1において行った後、データ受信装置2の鍵受信モジュール16は、ステップS2において、タイマーでトリガをかけ、セッション鍵Ksの更新タイミングを知る。

【0100】続いて、データ受信装置2の鍵受信モジュール16は、ステップS3において、MACアドレスとセッション鍵Ksの対応表にある現在のセッション鍵Ksのフラグを更新する。データ受信装置の鍵受信モジュール16は、例えば、図9のMACアドレスとセッション鍵Ksの対応表を有しており、この対応表を参照して、現在のセッション鍵Ksのフラグ112を更新する。この更新処理により、上記のp s c 111の上位1ビットが反転される。例えば、p s cの上位ビットが「0」に反転される。

【0101】そして、データ受信装置2では、ステップS4において、そのp s cに基づいてそのセクションに含まれているIPデータグラムの復号化を行う。すなわち、p s cの上位ビットが「0」とされた場合には、データ受信装置2の鍵受信モジュール16は、これまで使用していたセッション鍵Ks_odd (p s cの上位ビットが「1」のとき使用されるセッション鍵Ks) からセッション鍵Ks_evenに変更し、復号化モジュール15ではこのセッション鍵Ks_evenにより復号化を行う。また、p s cの上位ビットが「1」とされた場合には、データ受信装置2の鍵受信モジュール16は、これまで使用していたセッション鍵Ks_even (p s cの上位ビットが「0」のとき使用されるセッション鍵Ks) からセッション鍵Ks_oddに変更し、復号化モジュール15ではこのセッション鍵Ks_oddにより復号化を行う。

【0102】そして、次のセッション鍵Ksの切替えのタイミングまでの間に、ステップS5において、データ送信装置1の鍵管理モジュール12では、次のセッション鍵Ksをマスター鍵Km124により暗号化してデータ受信装置2に転送する。

【0103】なお、暗号化されたセッション鍵Km (Ks)の転送は、衛星回線3又は双方向の通信回線39を使って伝送するが、その伝送の際のプロトコルについては、応答の伴うプロトコルを用い、例えばT C P / I P (Transmission Control Protocol/Internet Protocol

1) を使用する。これにより、データ送信装置 1 からデータ受信装置 2 へのセッション鍵 K s の伝送が確実に行われる。

【0104】そして、この転送処理の間に、ステップ S 6 において、データ受信装置 2 の鍵受信モジュール 1 6 は、図 9 に示す MAC アドレスのセッション鍵 K s の対照表の更新を行う。すなわち、以前使用していたセッション鍵 K s を、新しいセッション鍵 K s に書き換える処理を行う。

【0105】その後、ステップ S 7 において、データ受信装置 2 の鍵受信モジュール 1 6 は、対象とするデータ受信装置 2 に次のセッション鍵 K s が保持されたかを確認した後に、ステップ S 8 に進み、次のセッション鍵 K s に切り替える。ここで、ステップ S 8 以降ステップ S 1 3 までの処理は、p s c の上位ビットが「1」とされて、セッション鍵 K s_{odd} を復号化に使用するときの処理であって、上記ステップ S 7 から進む処理であり、また、上記ステップ S 1 において、データ受信装置 2 にて現在のセッション鍵 K s がセッション鍵 K s_{even} (p s c の上位ビットが「0」とされたときに実行される処理でもある。

【0106】上述したような手順により、データ送信装置 1 は、更新されるセッション鍵 K s を確実にデータ受信装置 2 に届けことができて、データ受信装置 2 では、2 つ所持するセッション鍵 K s を切替えを瞬時にし、データの取りこぼしもなくセッション鍵 K s による復号化を実現することができる。なお、伝送処理時間の許す範囲で、セッション鍵 K s 1 2 4 の更新頻度は柔軟に変更することが可能である。

【0107】以上のようにセッション鍵 K s がデータ送信装置 1 において逐次変更されている場合でも、データ受信装置 2 は、このように変更されるセッション鍵 K s によって暗号化されているデータの復号が可能である。

【0108】次に、データ送信装置 1 がデータを送信するまでの手順、及びデータ受信装置 2 がデータを受信したときの手順について説明する。データ送信装置 1 がデータを送信するまでの手順については、例えば、図 1 0 に示すフローチャートに従って実行している。そして、データ受信装置 2 がデータを受信してからの手順については、例えば、図 1 1 に示すフローチャートに従って実行している。

【0109】先ず、データ送信装置 1 がデータを送信するまでの手順については、ステップ S 2 1 において、データ送信装置 1 は、データ受信装置 2 に伝送する I P データグラムを、データ送信装置 1 自身又は双方間の通信経路 3 9 に繋がるインターフェースより、受け取る。また、インターネット 4 上からのアクセス情報に基づいて、情報センタの情報の提供を受け取る。

【0110】次にステップ S 2 2 において、データ送信装置 1 は、I P データグラムの宛先アドレスを見て、第

1 のプロトコルの宛先アドレスを知る。例えば、データ送信装置 1 は、当該データ送信装置 1 内に所持している図 1 2 に示すような I P アドレスと MAC アドレスの対応表からデータ受信装置 2 の第 1 のプロトコルでの宛先アドレスを知る。

【0111】そして、宛先アドレスを知ったデータ送信装置 1 は、その宛先アドレスをもとに上記セッションを作成する。ここで、データ送信装置 1 は、必要に応じてデータ部にビット 1 によるパディングを行い、データ部が 6 4 ビットの倍数になるようにする。

【0112】次に、ステップ S 2 3 において、例えば図 9 に示したような MAC アドレスとセッション鍵 K s の対応表から現在のセッション鍵 K s のフラグ 1 1 2 を見て、現在使用しているセッション鍵 K s 1 2 4 を取り出し、当該取り出したセッション鍵 K s により、上記図 4 の (c) に示すように、セクションのデータ部を暗号化する。その際、現在のセッション鍵 K s のフラグを見て、その内容を上記図 9 に示すセッションのヘッダ部の p s c 1 1 1 の上位 1 ビットに入れる。

【0113】次にステップ S 2 4 において、図 4 の (e) 乃至図 4 の (g) に示すように、このセクション全体 1 0 9 を分割して各 T S パケット 1 0 6, 1 0 7, 1 0 8 のペイロード部 P に入れ、当該 T S パケット 1 0 6, 1 0 7, 1 0 8 に予め定められた上記 P I D を付加し、さらに、第 2 のプロトコルの必要に応じてペイロード部 P を暗号化し、衛星回線 3 に送出する。

【0114】以上がデータ送信装置 2 がデータを送信するまでの手順である。そして、データ受信装置 2 では、上述のようにして衛星回線 3 に送出されたデータを受信する。

【0115】データ受信装置 2 は、先ず図 1 1 のステップ S 3 1 において、衛星回線 3 より受信した T S パケット 1 0 6, 1 0 7, 1 0 8 を第 2 のプロトコルに従って復号化し、セクション全体 1 0 9 を再構築する。

【0116】次に、ステップ S 3 2 において、データ受信装置 2 は、セクションの宛先アドレス (MAC アドレス) を取り出し、続いて、ステップ S 3 3 において、図 1 3 に示す MAC アドレスとセッション鍵 K s の対応表を参照して MAC アドレスが存在するか否かの判別処理を行う。すなわち、自己に送信が許可されているデータを格納しているものであるか否かの判別処理を行う。ここで、MAC アドレスがないことを確認した場合には、データ受信装置 2 は、ステップ S 3 4 に進み、そのデータの破棄の処理を行う。また、MAC アドレスがあることを確認した場合には、データ送信装置 2 は、ステップ S 3 5 に進み、セクションヘッダ部 1 0 3 より前記図 8 に示した p s c 1 1 1 を取り出す。そして、データ送信装置 2 は、その p s c 1 1 1 の上位 1 ビットから現在有効なセッション鍵 K s がどちらであるかを調べ、2 つのセッション鍵 K s から現在有効とされるセッション鍵 K

sを取り出す。

【0117】データ受信装置2は、このようにして取り出したセッション鍵Ksにより、ステップS36において、セッションデータ部104をTriple-DESにより復号化する。

【0118】そして、データ受信装置2は、ステップS37において、当該復号したデータからIPデータグラムを取り出す。例えば、IPデータグラムの取り出しは、復号化されたデータ部の先頭にあるIPヘッダから図14のTOTAL LENGTH フィールド113を読み取り、IPデータグラムの長さを調べ、そこから計算されるIPデータグラム全体を取り出す。これにより、暗号化の際に付加した余計なパディングを除去される。このようにして目的とするIPデータグラムを取り出すことができる。

【0119】以上のような手順により、データ送信装置1は、データを送信するまでの処理を行い、また、データ受信装置2は、受信したデータに対する処理を行い、自己に宛てて配信されてきた情報データを受け取る。

【0120】なお、本実施の形態のデータサービスシステムは、次のように変形することも可能である。

【0121】すなわち、第1の変形例として、データサービスシステムは、図15に示すように構成することも可能である。この図15に示すデータサービスシステムは、データ受信装置2がIPルータとして構成される場合である。

【0122】ところで、上述したデータサービスシステムでは、データ受信装置2が直接IPデータグラムを受信する構成としている。しかし、このデータサービスシステムでは、データ受信装置2をIPルータとして構成することにより、データ受信装置2が衛星回線3から受信したデータを、イーサネットなどのローカルエリアネットワーク（LAN）202を経由してつながっている衛星回線3へのインターフェースを持たないコンピュータ203a、203bにもデータを伝送することができる。その際、データ送信装置1やデータ受信装置2は、データ受信装置2だけでなく、それがつながっているローカルエリアネットワーク202上のコンピュータ203a、203b全てについてのデータの配信を行うことができるようになる。具体的には、図12に示したデータ送信装置1内のIPアドレスとセクションの宛先アドレス（MACアドレス）の対応表のIPアドレスが、個別のIPアドレスではなく、複数のIPアドレスの集合を示すIPのネットワークアドレスに変換することになる。但し、このデータサービスシステムにおいて、データ伝送を行うのは衛星回線3の区間のみであるため、データ受信装置2とコンピュータ203a、203bの間でもデータ配信を行うには、IPプロトコル又はそれより上位のアプリケーションのレベルでのデータ配信制御が必要となる。

【0123】次に、第2の変形例として、データサービスシステムは、図16に示すように構成することも可能である。このデータサービスシステムでは、データ受信装置2がブリッジとして構成され、IPデータグラムを伝送するプロトコルの変換を行い、上記データ伝送システム201とは、ルーティングを行わないことで異なる。

【0124】この場合の上記データ受信装置2は、衛星回線3より受信したデータを復号化してIPデータグラムを取り出し、それをイーサネットフレームに入れて汎用のルータ302に転送する。そして、汎用のルータ302が、通常のIPデータグラムに対する処理を行う。これにより、ルーティングを行わないためにデータ受信装置2の構成が簡単になり、既存の汎用のルータを用いることができるようになる。

【0125】

【発明の効果】以上の説明で明らかなように、本発明においては、データを暗号化して提供し、暗号化されたデータの当該暗号化を解くための暗号鍵を管理し、暗号鍵を配信し、暗号鍵の配信形態に応じて課金を管理することにより、例えば衛星放送やデジタルCATV回線のような大容量で高速なデータ回線を使用してデータサービスを行う場合において、データの秘密性を維持しつつデータ単位やデータ種別毎の課金、更には契約者毎の課金を実現可能としている。

【0126】すなわち本発明のデータ伝送システムの課金方法及び装置は、例えば衛星放送や双方向或いは一方のデジタルCATV回線等の大容量且つ高速のデータ伝送路と、電話回線やISDN等に代表される比較的低速度の回線とを組み合わせることにより、高速のインターネットアクセス等のデータサービスを実現すると共に、IPパケットベースの暗号化における鍵配信の仕組みとデータ提供に対する課金とを組み合わせることにより、データの秘密性を維持しつつデータ単位やデータ種別毎の課金、更には契約者毎の課金を実現可能としている。

【図面の簡単な説明】

【図1】本発明のデータ伝送システムの課金方法及び装置が適用されるデータサービスシステムの主要部の構成を示すブロック図である。

【図2】本実施の形態のデータサービスシステムの顧客管理モジュールの構成例を示すブロック図である。

【図3】本発明の実施の形態であるデータサービスシステムの概略的な構成を示す図である。

【図4】本実施の形態のデータサービスシステムを構成するデータ送信装置からデータ受信装置へ送信されるデータであって、複数のプロトコルによってカプセル化が施されたデータを示す図である。

【図5】TSパケットのデータ構造のフォーマットを示す図である。

【図6】データ送信装置及びデータ受信装置の構成を示すブロック図である。

【図7】データ送信装置からデータ受信装置へ送信されるデータを暗号化するセッション鍵の変更を行う手続きの一連の工程を示すフローチャートである。

【図8】セクションヘッダのデータ構造を示す図である。

【図9】MACアドレスとセッション鍵のフラグとの対応表を示す図である。

【図10】データ送信装置において行うデータのカプセル化の一連の手続きを示すフローチャートである。

【図11】データ受信装置が受信したデータをセッション鍵により復号化するときの一連の手続きを示すフローチャートである。

【図12】IPアドレスとMACアドレスとの対応表を示す図である。

【図13】MACアドレスとセッション鍵の対応表を示す図である。

【図14】IPデータグラムの取り出しの際に使用されるTOTALLENGTHフィールドが格納されるデータ構造を示す図である。

す図である。

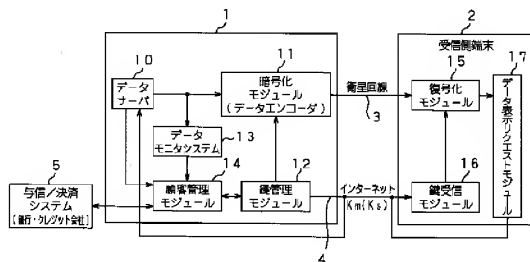
【図15】本実施の形態のデータサービスシステムの第1の変形例を示す図である。

【図16】本実施の形態のデータサービスシステムの第2の変形例を示す図である。

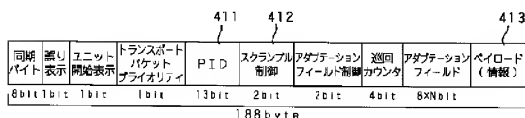
【符号の説明】

1 データ伝送装置、 2 受信側端末（データ受信装置）、 3 衛星回線、 4 インターネット、 5 与信/決済システム、 10 データサーバ、 11 暗号化モジュール（データエンコーダ）、 12 鍵管理モジュール、 13 データモニタモジュール、 14 顧客管理モジュール、 15 復号化モジュール、 16 鍵受信モジュール、 17 データ表示リクエストモジュール、 20 コンテンツ管理サーバ、 21 顧客データベース、 22 コンテンツ誤金設定部、 23 顧客認証/鍵管理モジュール制御部、 24 利用履歴ログ収集部、 25 利用料課金処理部、 26 請求・収納・支払・滞納管理部、 Ks セッション鍵、 Km マスター鍵

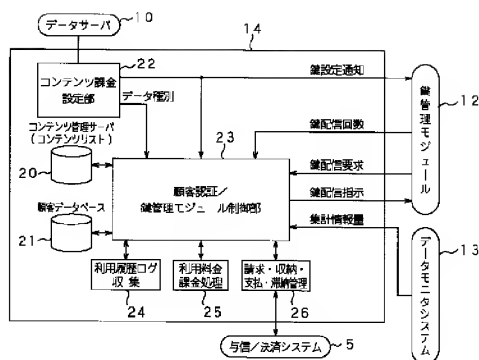
【図1】



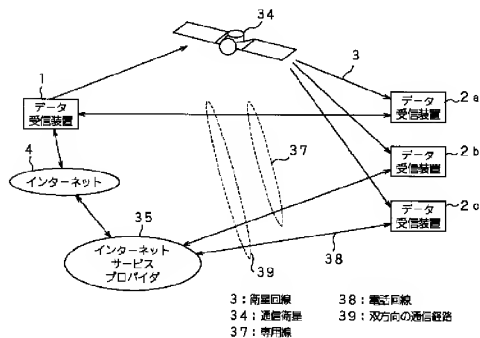
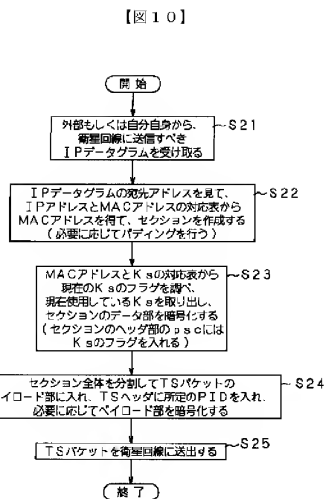
【図5】



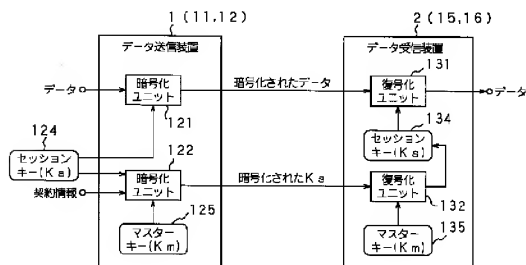
【図2】



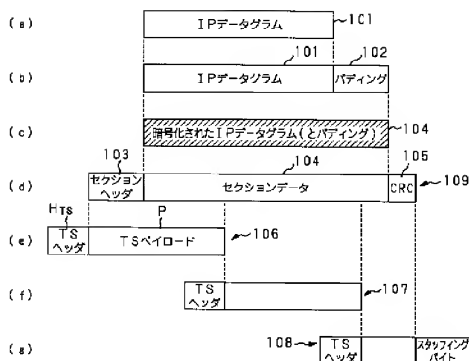
【図3】



【図6】



【図4】



【図8】

0	8	15	24	31
table_id	ssi	ai	rvd	section_length
MAC_address_5	rvd	psc	asc	section_number
MAC_address_4	MAC_address_3	MAC_address_2	MAC_address_1	last_section_number

ssi: section_syntax_indicator
 ai: private_indicator
 rvd: reserved
 psc: payload_scramble_indicator
 asc: address_scramble_indicator
 LSF: LLC_SNAP_flag
 onl: current_next_indicator

【図9】

【図12】

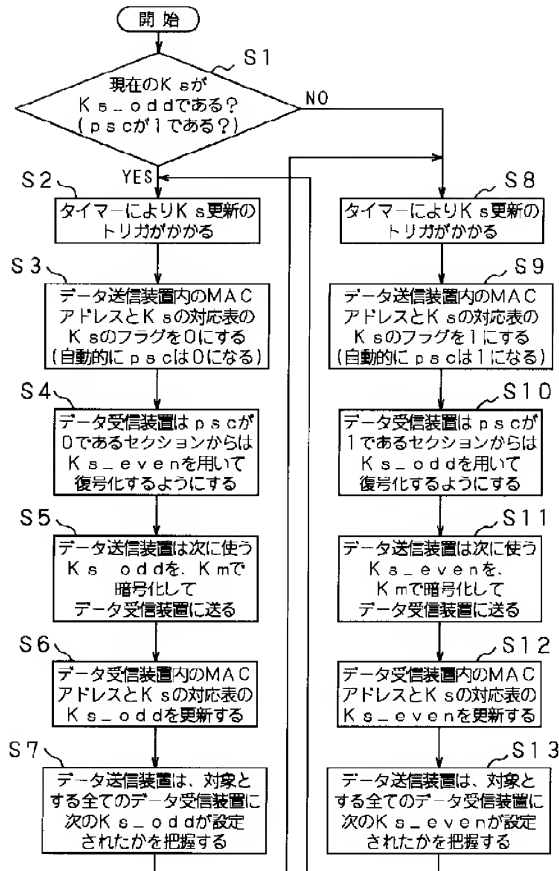
MACアドレス	Ks_even	Ks_odd	Ksフラグ
08:00:46:01:07:24	0xC08F...25	0x90B3...AF	0
08:00:46:01:07:09	0x26D2...61	0xBA02...3C	1
01:00:5e:16:0:0	0x461E...67	0xDC1A...22	0

IPアドレス	bitmask	MAC address
133.11.9.39	255.255.255.225	08:00:46:01:07:24
133.11.20.0	255.255.255.0	08:00:46:01:07:09
226.0.0.0	255.255.255.224	01:00:5e:16:0:0

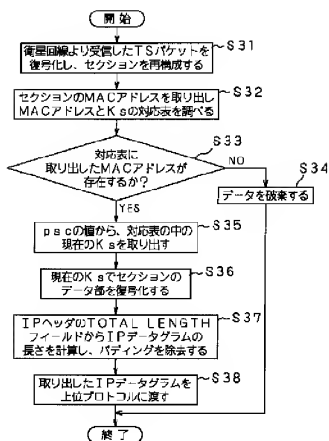
【図13】

MACアドレス	Ks_even	Ks_odd
08:00:46:01:07:24	0xC08F...25	0x90B3...AF
01:00:5e:16:0:0	0x461E...67	0xDC1A...22

【図 7】



【図11】

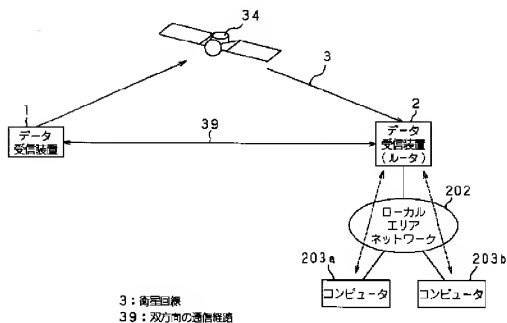


【図14】

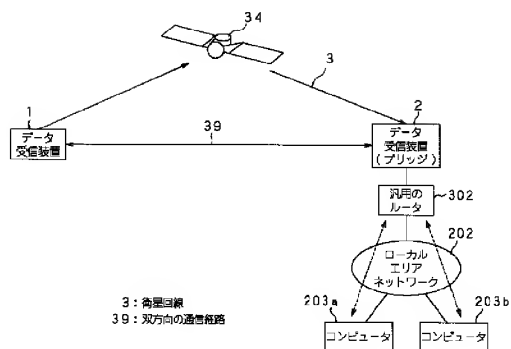
113

VERS	HLEN	SERVIE TYPE	TOTAL LENGTH
IDENTIFICATION		FLAGS-FRAGMENT OFFSET	
TIME TO LIVE	PROTOCOL	HEADER CHECKSUM	
SOURCE IP ADDRESS			
DESTINATION IP ADDRESS			
IP OPTIONS (IF ANY)		PADDING	
DATA			
...			

【図15】



【図16】



JP2000196673A HYBRID MOBILE COMMUNICATION SYSTEM, HYBRID MOBILE COMMUNICATION EQUIPMENT AND HYBRID MOBILE COMMUNICATING METHOD

Bibliography

DWPI Title

Hybrid mobile communication system e.g. speech communication system, adds address of wide range wireless base station to CSG and ASG data packets

Original Title

HYBRID MOBILE COMMUNICATION SYSTEM, HYBRID MOBILE COMMUNICATION EQUIPMENT AND HYBRID MOBILE COMMUNICATING METHOD

Assignee/Applicant

Standardized: TOSHIBA CORP

Original: TOSHIBA CORP

Inventor

TOSHIMITSU KIYOSHI ; SAKAMOTO TAKEFUMI; NOUJIN KATSUYA ; MORIYA OSAMU

Publication Date (Kind Code)

2000-07-14 (A)

Application Number / Date

JP1998374121A / 1998-12-28

Priority Number / Date / Country

JP1998374121A / 1998-12-28 / JP

Abstract

PROBLEM TO BE SOLVED: To enable efficient information transfer in a mobile communication system with a hybrid configuration.

SOLUTION: A CSG (control channel) packet forming part 15 and an ASG (access channel) packet forming part 16 make information transmitted through a CSG and an ASG a packet, and a wideband radio base station destination address setting part 13 adds the address of a wideband radio base station. Also, a USG (user information) adds the address of a server in a server destination address setting part 12. The CSG, ASG and USG to which addresses are added are converted to transmission signals to a two-way radio base station by a PPP(point-to-point protocol) forming part 7, a PIAFS(PHS Internet access forum standard) forming part 8 and a PHS(personal handy phone system) forming part 9 and transmitted. The user information is directly transmitted to a server to reduce useless traffic on a network.

(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号

特開2000-196673

(P2000-196673A)

(43) 公開日 平成12年7月14日 (2000.7.14)

(51) Int.Cl. ⁷	識別記号	F I	テマート* (参考)
H 0 4 L 12/56		H 0 4 L 11/20	1 0 2 Z 5 K 0 3 0
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 B 5 K 0 3 3
H 0 4 L 12/46		H 0 4 L 11/00	3 1 0 C 5 K 0 6 7
12/28		11/20	B
12/66			

審査請求 未請求 請求項の数9 O L (全 11 頁)

(21) 出願番号	特願平10-374121	(71) 出願人	000003078 株式会社東芝 神奈川県川崎市幸区堀川町72番地
(22) 出願日	平成10年12月28日 (1998. 12. 28)	(72) 発明者	利光 清 神奈川県川崎市幸区小向東芝町1 番地 株 式会社東芝研究開発センター内
		(72) 発明者	坂本 岳文 神奈川県川崎市幸区小向東芝町1 番地 株 式会社東芝研究開発センター内
		(74) 代理人	100076233 弁理士 伊藤 進

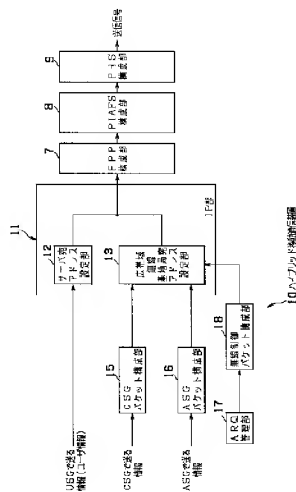
最終頁に続く

(54) 【発明の名称】 ハイブリッド移動通信システム、ハイブリッド移動通信装置及びハイブリッド移動通信方法

(57) 【要約】

【課題】 ハイブリッド構成の移動通信システムにおいて効率的な情報転送を可能とする。

【解決手段】 CSGパケット構成部15及びASGパケット構成部16は、CSG、ASGで伝送する情報をパケット化し、広帯域無線基地局宛アドレス設定部13によって広帯域無線基地局のアドレスを付加する。また、USG (ユーザ情報) はサーバ宛アドレス設定部12においてサーバのアドレスを付加する。アドレスが付加されたCSG、ASG、USGはPPP構成部7、PIAFS構成部8及びPHS構成部9によって双方向無線基地局に対する送信信号に変換されて送出される。ユーザ情報はサーバに直接伝送され、ネットワーク上の無用なトラフィックが低減される。



【特許請求の範囲】

【請求項1】 広帯域の第1の無線回線を用いて無線端末装置へ送信を行う第1の無線基地局と、
狭帯域の第2の無線回線を用いて前記無線端末装置との間で送受信を行う第2の無線基地局と、
前記第1の無線基地局と前記第2の無線基地局との間を接続するネットワーク上に設けられ、前記無線端末装置のユーザ情報を保持するサーバとを具備し、
前記無線端末装置は、前記ユーザ情報の宛先は、前記サーバ宛とし、前記第1の無線回線用の無線制御情報の宛先は、前記第1の無線基地局宛として送信することを特徴とするハイブリッド移動通信システム。

【請求項2】 広帯域の第1の無線回線を用いて送信を行う第1の無線基地局からの信号を受信する広帯域受信手段と、
狭帯域の第2の無線回線を用いて送受信を行う第2の無線基地局との間で信号の送受を行う狭帯域送受信手段と、
前記第1の無線基地局及び第2の無線基地局との間を接続するネットワーク上に設けられたサーバに対するユーザ情報をパケット化するユーザ情報パケット化手段と、
前記第1の無線回線用の無線制御情報をパケット化する制御情報パケット化手段と、
前記制御情報パケット化手段の出力に前記第1の無線基地局のアドレスを付加する第1の無線基地局アドレス付加手段と、
前記ユーザ情報パケット化手段の出力に前記サーバのアドレスを付加するサーバアドレス付加手段と、
前記第1の無線基地局アドレス付加手段及び前記サーバアドレス付加手段の出力を前記第2の無線基地局に送出するためのフォーマット変換を行って出力する送出手段とを具備したことを特徴とするハイブリッド移動通信装置。

【請求項3】 広帯域の第1の無線回線を用いて送信を行う第1の無線基地局及び狭帯域の第2の無線回線を用いて送受信を行う第2の無線基地局との間の通信を可能にするネットワーク上に設けられたサーバに対するユーザ情報をパケット化すると共に、前記第1の無線回線用の無線制御情報をパケット化するパケット化手順と、
パケット化された前記無線制御情報に前記第1の無線基地局のアドレスを付加し、パケット化された前記ユーザ情報に前記サーバのアドレスを付加するアドレス付加手順と、
アドレスが付加された前記無線制御情報及びユーザ情報を、前記第2の無線基地局に送出するためのフォーマット変換を行って出力する送出手順とを具備したことを特徴とするハイブリッド移動通信方法。

【請求項4】 前記無線端末装置は、前記第1の無線基地局を介して受信したユーザ情報パケットの送達確認用

の受信シーケンス番号の情報を前記第1の無線基地局を宛先として送出することを特徴とする請求項1に記載のハイブリッド移動通信システム。

【請求項5】 前記無線端末装置は、前記第1の無線基地局を介して受信したユーザ情報パケットの送達確認用の受信シーケンス番号の情報を前記制御情報として前記第1の無線基地局を宛先として送出することを特徴とする請求項1に記載のハイブリッド移動通信システム。

【請求項6】 前記第1の無線基地局を介して受信したユーザ情報パケットの送達確認用の受信シーケンス番号の情報を前記第1の無線基地局のアドレスを付加して前記送出手段に供給する無線制御パケット付加手段を更に具備したことを特徴とする請求項2に記載のハイブリッド移動通信装置。

【請求項7】 前記制御情報パケット化手段は、前記第1の無線基地局を介して受信したユーザ情報パケットの送達確認用の受信シーケンス番号の情報をパケット化することを特徴とする請求項2に記載のハイブリッド移動通信装置。

【請求項8】 前記第1の無線基地局を介して受信したユーザ情報パケットの送達確認用の受信シーケンス番号の情報を前記第1の無線基地局のアドレスを付加した後前記送出手順を行わせる無線制御パケット付加手順を更に具備したことを特徴とする請求項3に記載のハイブリッド移動通信方法。

【請求項9】 前記パケット化手順は、前記第1の無線基地局を介して受信したユーザ情報パケットの送達確認用の受信シーケンス番号の情報を制御情報としてパケット化することを特徴とする請求項3に記載のハイブリッド移動通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、狭帯域な通信路を有する移動通信システムと広帯域な通信路を有する移動通信システムを併用したハイブリッド移動通信システム、ハイブリッド移動通信装置及びハイブリッド移動通信方法に関する。

【0002】

【従来の技術】近年、移動通信システムの開発が進められている。既存の移動通信システムでは音声通信が主流であったが、情報通信にも利用可能な新たな移動通信システムの研究も進められている。また、次世代マルチメディア移動通信システムとして、既存の移動通信システムと新たな移動通信システムとを組み合わせたシステムも提案されている。

【0003】マルチメディアを扱う通信やインターネット上の通信、例えばWWWのようなアプリケーションでは、ユーザが発する情報量よりもユーザが受信する情報量の方が極めて大きい。従って、無線を介してデータ通信やインターネットと接続する場合には、上り無線チ

ヤネル(端末局から基地局方向)よりも、下り無線チャネル(基地局から端末局方向)の伝送速度を高速にすることで、無線端末局の送信電力を低減することができ、無線端末局の低消費電力化及び無線端末局の小型化が可能になる。

【0004】このような情報通信の利用形態を考慮して、上りの伝送速度を低速に構成し、下りの伝送速度を高速に構成する上下非対称なシステムが注目されている。例えば、既存移動通信システムとしてPHS(Personal Handy phone System)を利用し、新たに高速ダウンリンクを付加して情報提供サービスを行うシステムが提案されている。

【0005】高速ダウンリンクには、例えば、MMAC(Multimedia Mobile Access Communication: マルチメディア移動アクセス推進協議会)で提案されている広帯域無線システムのダウンリンクのみを利用する方法がある。図11はこのようなハイブリッド移動通信システムの構成を示す説明図である。

【0006】図11において、ネットワーク2にはサーバ1が接続されている。サーバ1には利用者に提供する情報が蓄積されており、ネットワーク2はサーバ1に蓄積されている情報を伝送することができる。ネットワーク2には、PHS基地局(以下、CS(Cell Station))という3及び広帯域無線システム用基地局(以下、AP(Access Point))という5も接続されており、PHS基地局3は無線端末局4との間で無線による通信が可能である。

【0007】無線端末局4はPHSを用いてCS3との間で情報の送受が可能である。また、無線端末局4はAP4から送信された情報を受信することが可能である。無線端末局4とCS3との通信速度よりも無線端末局4とAP5との間の通信速度の方が高速である。

【0008】無線端末局4はサーバ1から情報をダウンロードすることができる。次に、無線端末局4が情報をサーバ1に要求し受信する手順例を示す。

【0009】無線端末局4は情報要求信号をPHSを用いてCS3に対して送信する。情報要求信号は、CS3からネットワーク2を介してサーバ1に届けられる。情報要求信号を受信したサーバ1は、情報要求に基づいて、無線端末局4宛てに要求された情報を送信する。この情報はネットワーク2を介してAP4に届けられ、AP4はこの情報を無線端末局4に送信する。

【0010】このような動作により、画像情報や音声情報等を含む大容量の情報を短時間で無線端末局4に送信することが可能となる。移動環境におけるマルチメディアサービスは端末局での大容量情報の受信が中心になると考えられる。図11に示すように、PHS等の既存の移動通信システムに高速送信可能な移動通信システムを新たに付加することで、移動環境において大部分のマルチメディアサービスを無線端末局に対して提供すること

が可能となる。

【0011】また、図11の構成では、無線端末局4には、AP5にデータを送信するための高速送信機は不要である。無線端末局4の送信系としては、既存の移動通信システムを利用することができ、端末局の低コスト化、低消費電力化及び小型化を図ることが可能となる。更に、新たな移動通信システムを導入する初期段階では、サービスエリアが局所的になるものと考えられるが、既存の移動通信システムを併用することにより、低速ではあるものの広い範囲でのサービスの提供が可能となる。

【0012】このように、上り無線チャネルとして既存の移動通信システム、例えばPDCやPHS等の上りチャネルを使用し、下りは別の高速な無線チャネルを用いた非対称の無線システムは、高速且つ安価なシステムとして注目されている。

【0013】しかしながら、上述した非対称通信システムを実現するために、APと無線端末局間の無線回線を維持する必要があり、無線端末局はCSを介してAPに無線回線制御情報を伝送しなければならないが、効率的な伝送方法については考えられていない。

【0014】

【発明が解決しようとする課題】このように、従来、ハイブリッド構成の移動通信システムにおいては、広帯域無線システムを利用した無線回線を維持するための無線回線制御情報の効果的な伝送方法は存在しないという問題点があった。

【0015】本発明は、狭帯域な双方向通信路を持つ無線通信システムと広帯域な下り片方向通信路を持つ無線通信システムを併用したハイブリッド構成の移動通信システムにおいて効率的な情報転送を可能とすることができるハイブリッド移動通信システム、ハイブリッド移動通信装置及びハイブリッド移動通信方法を提供することを目的とする。

【0016】

【課題を解決するための手段】本発明の請求項1に係るハイブリッド移動通信システムは、広帯域の第1の無線回線を用いて無線端末装置へ送信を行う第1の無線基地局と、狭帯域の第2の無線回線を用いて前記無線端末装置との間で送受信を行う第2の無線基地局と、前記第1の無線基地局と前記第2の無線基地局との間を接続するネットワーク上に設けられ、前記無線端末装置のユーザ情報を保持するサーバとを具備し、前記無線端末装置は、前記ユーザ情報の宛先は、前記サーバ宛とし、前記第1の無線回線用の無線制御情報の宛先は、前記第1の無線基地局宛として送信するものであり、本発明の請求項2に係るハイブリッド移動通信装置は、広帯域の第1の無線回線を用いて送信を行う第1の無線基地局からの信号を受信する広帯域受信手段と、狭帯域の第2の無線回線を用いて送受信を行う第2の無線基地局との間で信

号の送受を行う狭帯域送受信手段と、前記第1の無線基地局及び第2の無線基地局との間を接続するネットワーク上に設けられたサーバに対するユーザ情報をパケット化するユーザ情報パケット化手段と、前記第1の無線回線用の無線制御情報をパケット化する制御情報パケット化手段と、前記制御情報パケット化手段の出力に前記第1の無線基地局のアドレスを付加する第1の無線基地局アドレス付加手段と、前記ユーザ情報パケット化手段の出力に前記サーバのアドレスを付加するサーバアドレス付加手段と、前記第1の無線基地局アドレス付加手段及び前記サーバアドレス付加手段の出力を前記第2の無線基地局に送出するためのフォーマット変換を行って出力する送出手段とを具備したものであり、本発明の請求項3に係るハイブリッド移動通信方法は、広帯域の第1の無線回線を用いて送信を行う第1の無線基地局及び広帯域の第2の無線回線を用いて送受信を行う第2の無線基地局との間の通信を可能にするネットワーク上に設けられたサーバに対するユーザ情報をパケット化すると共に、前記第1の無線回線用の無線制御情報をパケット化するパケット化手順と、パケット化された前記無線制御情報に前記第1の無線基地局のアドレスを付加し、パケット化された前記ユーザ情報に前記サーバのアドレスを付加するアドレス付加手順と、アドレスが付加された前記無線制御情報及びユーザ情報を、前記第2の無線基地局に送出するためのフォーマット変換を行って出力する送出手段とを具備したものである。

【0017】本発明の請求項1において、無線端末装置からの第1の無線回線用の無線制御情報は第1の無線基地局を宛先とし、ユーザ情報はサーバを宛先として、第2の無線基地局に送信される。ユーザ情報が第1の無線基地局に送信されないで、(有線)ネットワーク上の無用なトラフィックが低減される。サーバからの情報は第1の無線基地局から無線端末装置に伝送される。

【0018】本発明の請求項2において、第1の無線回線用の無線制御情報は制御情報パケット化手段によってパケット化され、ユーザ情報はユーザ情報パケット化手段によってパケット化される。パケット化された無線制御情報は第1の無線基地局のアドレスが付加され、第2の無線基地局に対応したフォーマットで送出される。また、パケット化されたユーザ情報はサーバのアドレスが付加され、第2の無線基地局に対応したフォーマットで送出される。

【0019】本発明の請求項3において、第1の無線回線用の無線制御情報とユーザ情報はパケット化された後、無線制御情報には第1の無線基地局のアドレスが付加され、ユーザ情報にはサーバのアドレスが付加される。アドレスが付加された制御情報及びユーザ情報は第2の無線基地局に送出するためにフォーマット変換されて送出される。

【0020】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について詳細に説明する。図1は本発明に係るハイブリッド移動通信装置の一実施の形態を示すブロック図である。図1は無線端末局を構成するハイブリッド移動通信装置10を示している。図2は図1のハイブリッド移動通信装置10によって構成される無線端末局25を含む無線通信システムの全体構成を概略的に示す説明図である。

【0021】図2において、ネットワーク21には、1又は複数の広帯域無線基地局23、1又は複数の双方向通信無線基地局24及びサーバ22が接続されており、相互に通信可能となっている。また、無線端末局25は、広帯域無線基地局23が送信した情報を受信することができると共に、双方向通信無線基地局24との間で情報の送受信が可能となっている。つまり、無線端末局25及び双方向通信無線基地局24相互間(双方向無線リンク)は、双方向の無線回線が構築され、無線端末局25及び広帯域無線基地局23相互間(広帯域無線リンク)は、ダウンリンクのみの単方向の無線回線が構築される。

【0022】ところで、図2では、単一のネットワーク21に広帯域無線基地局23及び双方向通信無線基地局24が接続されている場合について示しているが、広帯域無線基地局23と双方向通信無線基地局24とを収容するネットワークが夫々異なり、異なるネットワークが中継局によって接続される構成も考えられる。

【0023】図3はこのような場合の無線通信システムの全体構成を概略的に示す説明図である。

【0024】図3において、2つのネットワーク21A、21Bは中継局26によって接続されている。ネットワーク21Aは広帯域無線基地局23を収容するネットワークであり、ネットワーク21Bは双方向通信無線基地局24を収容するネットワークである。サーバ22の位置は、接続可能であればいずれのネットワーク上であってもよく、ネットワーク21A、21Bに接続可能な図示しない他のネットワーク上であっても構わない。図3では、便宜上、サーバ22がネットワーク21A上に存在する場合を示す。

【0025】広帯域無線リンクと双方向無線リンクを利用したハイブリッド構成の無線システムでは、広帯域無線リンクを維持するための無線回線制御情報を双方向無線リンクを介して伝送しなければならない。例えば、無線端末局25が広帯域無線基地局23から、広帯域無線リンク用の無線データリンク制御情報を受信した場合には、その応答信号は、双方向無線リンクを介して伝送しなければならない。特に、既存の双方向無線リンクを利用した場合を想定すると、双方向無線リンクから見れば、ユーザ情報と同様な扱いで広帯域無線リンク用の無線データリンク情報を伝送しなければならない。

【0026】図1のハイブリッド移動通信装置10は、